aws

Guide du développeur

Amazon CloudFront



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon CloudFront: Guide du développeur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'Amazon CloudFront ? 1
Comment vous configurez-vous CloudFront pour diffuser du contenu 2
Choix entre une distribution standard ou une distribution multi-locataires 5
Tarification 5
Façons d'utiliser CloudFront 6
Accélération de la diffusion de contenu de site web statique 6
Diffusion de vidéo en streaming à la demande et en direct 6
Chiffrement de champs spécifiques tout au long du traitement du système 7
Personnalisation au niveau de l'emplacement périphérique 7
Diffusion de contenu privé à l'aide des personnalisations de Lambda@Edge 8
Comment CloudFront diffuse le contenu 8
Comment CloudFront diffuser du contenu à vos utilisateurs 9
Comment CloudFront fonctionne avec les caches périphériques régionaux 10
CloudFront serveurs Edge 13
Utiliser la liste de préfixes CloudFront gérée 13
Utilisation des AWS kits de développement logiciel 14
CloudFront ressources techniques 15
Prise en main 16
Configurez votre Compte AWS 16
Inscrivez-vous pour un Compte AWS 17
Choisissez le mode d'accès CloudFront 17
Mise en route avec une distribution standard 17
Conditions préalables 18
Création d’un compartiment 18
Chargement du contenu 19
Création d’une distribution 20
Accès au contenu 21
Nettoyage 22
Amélioration de votre distribution de base 22
Commencer (AWS CLI) 22
Conditions préalables 23
Créer un compartiment Amazon S3 23
Chargement du contenu dans le compartiment 24
Création d’un contrôle d’accès d’origine (OAC) 24

Création d'une distribution standard 24
Mise à jour de votre stratégie de compartiment S3 26
Confirmation du déploiement de la distribution 27
Accédez à votre contenu via CloudFront 27
Nettoyage 28
Mise en route avec un site web statique sécurisé 29
Présentation de la solution 30
Déploiement de la solution 31
E-commerce distributions 37
Présentation de l'architecture 37
Comportements du cache pour le commerce électronique 38
Stratégie TTL pour le contenu du marché 40
Configuration d'origine 41
Amazon S3 Origin pour les actifs statiques 41
Origine ALB pour le contenu dynamique 42
Application-level mise en cache avec ElastiCache (Valkey) 43
Questions fréquentes (FAQ) 44
Comment gérer le contenu personnalisé grâce à la mise en cache ? 45
Comment choisir entre l'invalidation et les TTL courts ? 45
Comment me préparer aux ventes flash et aux pics de trafic ? 45
Dois-je utiliser Origin Shield pour mon site de vente ? 45
E-commerce liste de contrôle de sécurité 46
URL signées et cookies pour le contenu premium 46
Contrôle d'accès à l'origine (OAC) pour Amazon S3 47
Chiffrement en transit 48
Groupes de sécurité VPC pour le cluster de cache 49
Contrôles de sécurité supplémentaires 50
CloudFront plans tarifaires forfaitaires 51
Avantages des plans tarifaires CloudFront forfaitaires 52
Fonctionnalités par niveau de plan tarifaire 52
Caractéristiques du plan tarifaire 53
Allocations d'utilisation mensuelles 99
Qu'est-ce qui compte pour votre allocation d'utilisation 100
Que se passe-t-il lorsque l'utilisation dépasse l'allocation 100
Allocations d'utilisation configurables sur le plan Premium 101
Éligibilité basée sur l'utilisation historique 102

Coûts couverts par votre plan 103
La gestion du DNS Route 53 et votre plan 103
Réduire globalement AWS coûts liés aux plans tarifaires 105
Gérez vos plans tarifaires forfaitaires 105
Souscrire une nouvelle distribution à un plan tarifaire 106
Souscrire une distribution existante à un plan tarifaire 106
Mettre à niveau un plan tarifaire 107
Modifier le niveau d'utilisation de votre forfait Premium 107
Rétrograder un plan tarifaire 108
Annuler un plan tarifaire 109
Annuler un changement de plan en cours 109
Supprimer une distribution avec un plan tarifaire 110
Permissions 110
Flat-rate quotas de plans tarifaires 110
Fonctions non prises en charge 111
Fonctions non prises en charge 111
Associations non soutenues 113
Account-level contraintes 114
Resource-level contraintes 114
Fonctionnalités supplémentaires susceptibles d'affecter votre plan tarifaire 114
Plans tarifaires par rapport à la tarification à l'utilisation 116
Configuration des distributions 117
Compréhension du fonctionnement des distributions multi-locataires 119
Comment ça marche 120
Termes 122
Fonctions non prises en charge 124
Personnalisations du locataire de distribution 125
Demande de certificats (locataire de distribution) 129
Création d’un groupe de connexions personnalisé (facultatif) 138
Migration vers une distribution multi-locataires 140
Créer une distribution 141
Création d'une CloudFront distribution dans la console 143
Valeurs affichées 149
Liens supplémentaires 150
Ajoutez un domaine à votre distribution CloudFront standard 150
Paramètres de distribution préconfigurés 153

Origine Amazon S3 153
Origine API Gateway 155
Origine personnalisée et instance EC2 156
origine Elastic Load Balancing 158
MediaPackage origine v1 160
MediaPackage origine v2 161
MediaTailor origine 162
Tous les paramètres de distribution 163
Paramètres d'origine 163
Paramètres de comportement du cache 175
Paramètres de distribution 191
Pages d'erreur personnalisées et mise en cache des erreurs 202
Restrictions géographiques 203
Test d'une distribution 203
Création de liens vers vos objets 204
Mettre à jour une distribution 205
Mise à jour d'une distribution dans la console 205
Marquer une CloudFront ressource 208
Restrictions liées aux étiquettes 209
Baliser vos ressources pour facturation 210
Ajouter, modifier et supprimer des balises 210
Balisage par programmation 211
Supprimer une distribution 211
Utilisation de différentes origines 214
Utilisation d'un compartiment Amazon S3 215
Utiliser un MediaStore conteneur ou un MediaPackage canal 228
Utilisation d'un Application Load Balancer 228
Utilisation d'un Network Load Balancer 229
Utilisation d'une URL de fonction Lambda 229
Utilisez un AWS Lambda Fonction Web 231
Utilisation d'Amazon EC2 (ou autre origine personnalisée) 232
Utiliser des groupes CloudFront d'origine 234
Utilisation d'Amazon API Gateway 234
Activation d'IPv6 234
Demandes utilisateur en IPv6 235
Demandes d'origine en IPv6 236

Utilisation du déploiement continu pour tester en toute sécurité les changements 237
CloudFront flux de travail de déploiement continu 239
Utilisation d'une distribution intermédiaire et d'une politique de déploiement continu 240
Surveillance d'une distribution intermédiaire 251
Découvrez le fonctionnement du déploiement continu 251
Quotas et autres considérations relatives au déploiement continu 254
Utilisation d'URL personnalisées 255
Exigences relatives à l'utilisation de noms de domaines alternatifs 256
Restrictions relatives à l'utilisation de noms de domaines alternatifs 258
Ajout d'un nom de domaine alternatif 261
Déplacement d'un nom de domaine alternatif 264
Suppression d'un nom de domaine alternatif 277
Utilisation des caractères génériques dans les noms de domaines alternatifs 278
Utiliser WebSockets 279
Comment fonctionne le WebSocket protocole 280
WebSocket exigences 280
WebSocket En-têtes recommandés 281
Demande d'adresses IP statiques en unidiffusion à utiliser pour la liste d'autorisation 281
Conditions préalables 282
Demande d'une liste d'adresses IP statique en unidiffusion 282
Création d'une liste d'adresses IP statiques en unidiffusion 283
Association d'une liste d'adresses IP statiques en unidiffusion à une distribution existante .. 283
Association d'une liste d'adresses IP statiques en unidiffusion à une nouvelle distribution ... 284
Associer une liste IP statique Anycast à un groupe de connexion 285
Mettre à jour une liste d'adresses IP statiques Anycast 286
Utilisez votre propre adresse IP pour CloudFront utiliser IPAM 286
Utilisation du framework gRPC 291
Comment fonctionne le gRPC dans CloudFront 292
Travailler avec des ressources partagées dans CloudFront 294
Conditions préalables au partage des ressources 294
Partage d'une origine VPC 295
Utilisation d'une origine VPC partagée 298
Identifier une origine VPC partagée 299
Annuler le partage d'une origine VPC partagée 299
Responsabilités et autorisations pour les origines de VPC partagées 300
Autorisations accordées aux propriétaires 300

Autorisations accordées aux consommateurs 300
AWSRAMDefaultPermissionCloudFront 300
Facturation et mesures 301
Quotas de ressources partagées 301
Mise en cache et disponibilité 302
Amélioration de votre taux d'accès au cache 303
Spécifiez la durée de mise CloudFront en cache de vos objets 303
Utilisation d'Origin Shield 303
Mise en cache basée sur les paramètres de chaîne de requête 304
Mise en cache basée sur des valeurs de cookie 304
Mise en cache basée sur des valeurs d'en-tête 306
Supprimer l'en-tête `Accept-Encoding` lorsqu'une compression n'est pas nécessaire 307
Diffusion de contenu multimédia via HTTP 307
Utilisation d'Origin Shield 307
Cas d'utilisation pour Origin Shield 309
Cliquez sur l'onglet AWS Région pour Origin Shield 314
Activer Origin Shield 316
Estimation des frais liés à Origin Shield 318
Haute disponibilité d'Origin Shield 319
Comment Origin Shield interagit avec les autres fonctionnalités CloudFront 320
Augmentation de la disponibilité avec le basculement d'origine 321
Création d'un groupe d'origine 323
Contrôle des délais d'expiration et des tentatives de l'origine 325
Utilisation du basculement d'origine avec les fonctions Lambda@Edge 326
Utilisation des pages d'erreur personnalisées avec le basculement d'origine 327
Gestion de l'expiration de cache 328
Utilisation des en-têtes pour contrôler la durée de conservation en cache pour des objets individuels 329
Diffusion de contenu obsolète (expiré) 331
Spécifiez la durée pendant laquelle les objets sont CloudFront mis en cache 333
Ajout d'en-têtes à vos objets à l'aide de la console Amazon S3 340
Mise en cache basée et paramètres de chaîne de requête 340
Paramètres de console et d'API pour le réacheminement et la mise en cache des chaînes de requête 343
Optimisation de la mise en cache 343
Paramètres de chaîne de requête et journaux CloudFront standard (journaux d'accès) 345

Mise en cache de contenu basée sur des cookies 345
Mise en cache de contenu basée sur des en-têtes de demandes 349
En-têtes et distributions web : présentation 349
Sélection des en-têtes sur lesquels baser la mise en cache 351
Configurer CloudFront pour respecter les paramètres CORS 352
Configuration de la mise en cache en fonction du type d'appareil 353
Configuration de la mise en cache en fonction de la langue de l'utilisateur 353
Configuration de la mise en cache en fonction de l'emplacement de l'utilisateur 353
Configuration de la mise en cache en fonction du protocole de la demande 354
Configuration de mise en cache pour les fichiers compressés 354
Incidence de la mise en cache basée sur les en-têtes sur les performances 354
Impact de la casse des en-têtes et des valeurs d'en-tête sur la mise en cache 354
En-têtes qui CloudFront renvoient au visualiseur 355
Contrôle de la clé de cache à l'aide d'une politique 356
Compréhension des politiques de cache 357
Informations sur les politiques 357
Paramètres time-to-live (TTL) 357
Paramètres de la clé de cache 358
Création de politiques de cache 365
Utilisation des politiques de cache gérées 370
Amplify 370
CachingDisabled 372
CachingOptimized 372
CachingOptimizedForUncompressedObjects 373
Élémentaire- MediaPackage 374
UseOriginCacheControlHeaders 375
UseOriginCacheControlHeaders-QueryStrings 376
Comprendre la clé de cache 377
Clé de cache par défaut 378
Personnalisation de la clé de cache 379
Contrôle des demandes d'origine à l'aide d'une stratégie 382
Compréhension des stratégies de demande d'origine 383
Informations sur les stratégies 383
Paramètres de la demande d'origine 383
Création de stratégies de demande d'origine 386
Utilisation des stratégies de demande d'origine gérées 391

AllViewer ... 391
AllViewerAndCloudFrontHeaders-2022-06 ... 392
AllViewerExceptHostHeader ... 393
CORS-CustomOrigin ... 394
CORS-S3Origin ... 394
Elemental-MediaTailor-PersonalizedManifests ... 395
HostHeaderOnly ... 396
UserAgentRefererHeaders ... 396
Ajouter des en-têtes de CloudFront demande ... 397
En-têtes de type d'appareil ... 398
En-têtes de l'emplacement de l'utilisateur ... 398
En-têtes permettant de déterminer la structure de l'en-tête de l'utilisateur ... 400
En-têtes liés à TLS ... 400
Autres CloudFront en-têtes ... 401
Comprendre comment les politiques de demande d'origine et les politiques de cache fonctionnent ensemble ... 402
Ajout ou suppression d'en-têtes de réponse à l'aide d'une politique ... 407
Comprendre les politiques d'en-têtes de réponses ... 408
Détails de la politique (métadonnées) ... 408
En-têtes CORS ... 409
En-têtes de sécurité ... 413
En-têtes personnalisés ... 415
Suppression d'en-têtes ... 415
Server-Timing en-tête ... 417
Création de politiques d'en-têtes de réponses ... 422
Utilisation de politiques d'en-têtes de réponse gérées ... 430
Cors-et- SecurityHeadersPolicy ... 430
CORS-With-Preflight ... 431
CORS- - with-preflight-and SecurityHeadersPolicy ... 432
SecurityHeadersPolicy ... 433
SimpleCORS ... 434
Comportement des demandes et des réponses ... 436
Comment CloudFront traiter les requêtes HTTP et HTTPS ... 436
Comportement des demandes et des réponses pour les origines Amazon S3 Origins ... 437
Comment CloudFront traiter et transférer les demandes vers votre origine Amazon S3 ... 437
Comment CloudFront traite les réponses provenant de votre Amazon S3 origin ... 444

Comportement des demandes et des réponses pour les origines personnalisées 447
Comment CloudFront traiter et transférer les demandes vers votre origine personnalisée 447
Comment CloudFront traite les réponses provenant de votre origine personnalisée 466
Comportement des requêtes et des réponses pour les groupes d'origine 471
Ajout d'en-têtes personnalisés aux demandes d'origine 472
Cas d'utilisation 472
Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine 473
En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine 474
Configurer CloudFront pour transférer l'`en-tête` d'autorisation 475
Comment les CloudFront processus varient selon les GET 476
Utiliser les demandes de plage pour mettre en cache de large objets 477
Comment CloudFront traite les codes d'état HTTP 3xx depuis votre origine 478
Comment CloudFront traite les codes d'état HTTP 4xx et 5xx depuis votre origine 479
Comment CloudFront traiter les erreurs lorsque vous avez configuré des pages d'erreur personnalisées 480
Comment traiter CloudFront les erreurs si vous n'avez pas configuré de pages d'erreur personnalisées 482
Codes d'état HTTP 4xx et 5xx qui mettent en cache CloudFront 485
Génération de réponses aux·erreurs personnalisées 486
Configuration du comportement de réponses aux·erreurs 487
Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques 489
Stockage des objets et des pages d'erreur personnalisées dans des emplacements différents 491
Modifier les codes de réponse renvoyés par CloudFront 492
Contrôlez la durée de mise en CloudFront cache des erreurs 493
Ajout, suppression ou remplacement du contenu 495
Ajout et accès au contenu 495
Utilisation de la gestion des versions de fichiers pour mettre à jour ou supprimer du contenu existant 496
Mise à jour des fichiers existants à l'aide de noms de fichiers versionnés 496
Supprimer du contenu pour CloudFront ne pas le diffuser 497
Personnalisation des URL de fichier 497
Utilisation de votre propre nom de domaine (exemple.com) 498
Utilisation d'une barre oblique (/) à la fin dans des URL 498
Création d'URL signées pour des contenus restreints 499

Spécification d’un objet racine par défaut 499
Comment spécifier un objet racine par défaut 499
Fonctionnement de l'objet racine par défaut 501
Comment CloudFront fonctionne si vous ne définissez pas d'objet racine 503
Invalidation de fichiers pour supprimer du contenu 503
Choix entre invalider des fichiers existants et utiliser des noms de fichier versionnés 504
Déterminez les chemins à invalider 505
Ce que vous devez savoir lorsque vous invalidez des chemins 505
Invalidation de contenu par des balises de cache 510
Ce que vous devez savoir lorsque vous invalidez des balises 515
Invalidation de fichiers 516
Paiement d’une invalidation de fichier 520
Diffusion de fichiers compressés 521
Configurer CloudFront pour compresser des objets 521
Comment fonctionne CloudFront la compression 522
Conditions de compression 523
Types de fichiers qui CloudFront compressent 525
Conversion de l'en-tête ETag 527
Utilisation AWS WAF protections 529
Enable AWS WAF pour les distributions 530
Enable AWS WAF pour une nouvelle distribution 530
Utilisation d'une ACL Web existante 531
Activation du contrôle des bots 532
Configuration de la protection par catégorie de bot 533
Gérez les protections AWS WAF de sécurité pour CloudFront 534
Conditions préalables 535
Enable AWS WAF journaux 535
Configuration de la limitation du débit 536
Désactiver AWS WAF protections de sécurité 537
Configuration d’un accès sécurisé et restriction de l’accès au contenu 539
Utilisez le protocole HTTPS avec CloudFront 540
Exiger le protocole HTTPS entre les spectateurs et CloudFront 541
Exigence du protocole HTTPS vers une origine personnalisée 544
Exigence du protocole HTTPS vers une origine Amazon S3 547
Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront 549
Protocoles et chiffrements pris en charge entre CloudFront et l'origine 558

Utilisation de noms de domaines alternatifs et HTTPS 560
Choisissez la manière dont CloudFront les requêtes HTTPS sont traitées 561
Exigences relatives à l'utilisation de SSL/TLS certificats avec CloudFront 565
Quotas d'utilisation de SSL/TLS certificats avec CloudFront (HTTPS entre spectateurs et CloudFront uniquement) 570
Configuration de noms de domaines alternatifs et HTTPS 572
Déterminer la taille de la clé publique dans un certificat SSL/TLS RSA 576
Augmenter les quotas de SSL/TLS certificats 577
Rotation SSL/TLS des certificats 578
Revenir d'un SSL/TLS certificat personnalisé au certificat par défaut CloudFront 579
Passez d'un SSL/TLS certificat personnalisé avec des adresses IP dédiées au SNI 581
Authentification TLS mutuelle avec CloudFront (Viewer MTLS) 582
Comment ça marche 582
Cas d’utilisation 583
Trust Stores et gestion des certificats 583
Activer le protocole TLS mutuel pour les distributions CloudFront 591
Associer une fonction CloudFront de connexion 595
Configuration de paramètres supplémentaires 601
En-têtes MTLS Viewer pour les politiques de cache et transférés à l'origine 603
Révocation du certificat 607
Méthodes auxiliaires pour le protocole TLS mutuel 616
Modes de validation supplémentaires 617
Observabilité à l'aide des journaux de connexion 621
TLS mutuel d'origine avec CloudFront 626
Viewer mTLS contre Origin mTLS 627
Comment ça marche 627
Cas d’utilisation 628
Important : configuration requise pour le serveur Origin 628
Prise en main 629
Gestion des certificats avec AWS Gestionnaire de certificats 629
Activer le protocole TLS mutuel d'origine pour les distributions CloudFront 633
Utilisation de CloudFront fonctions avec un TLS mutuel d'origine 637
Restriction de contenu avec des URL et des cookies signés 640
Comment diffuser du contenu privé 640
Restriction de l’accès aux fichiers 641
Spécification des signataires autorisés 644

Choix entre des URL signées et des cookies signés ... 654
Utilisation des URL signées ... 655
Utilisation de cookies signés ... 680
Utilisation d'une commande Linux et OpenSSL pour le chiffrement et l'encodage en base64 ... 712
Exemples de code pour les URL signées ... 713
Restreindre l'accès à un AWS origine ... 744
Restreindre l'accès à une origine AWS Elemental MediaPackage v2 ... 745
Restreindre l'accès à un AWS Elemental MediaStore origine ... 752
Restreindre l'accès à un AWS Lambda origine de l'URL de la fonction ... 760
Restreindre l'accès à un AWS Lambda Origine de la fonction Web ... 771
Restriction de l'accès à une origine Amazon S3 ... 778
Restriction de l'accès avec les origines de VPC ... 795
Restreindre l'accès à l'origine d'un point Multi-Region d'accès Amazon S3 ... 803
Restriction de l'accès aux Application Load Balancers ... 810
Configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes ... 811
Configuration d'un Application Load Balancer pour transférer uniquement les demandes contenant un en-tête spécifique ... 813
(Facultatif) Améliorer la sécurité de cette solution ... 815
(Facultatif) Limitez l'accès à l'origine en utilisant AWS-liste de préfixes gérée pour CloudFront ... 816
Restriction géographique ... 817
Utiliser des restrictions CloudFront géographiques ... 817
Utilisation d'un service de géolocalisation tiers ... 820
Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles ... 821
Présentation du chiffrement au niveau du champ ... 823
Configuration du chiffrement au niveau du champ ... 824
Déchiffrage de champs de données à votre origine ... 830
Vidéo streaming à la demande et en direct ... 834
À propos des vidéos streaming ... 834
Distribution de vidéos à la demande ... 835
Configuration de vidéo à la demande pour Microsoft Smooth Streaming ... 836
Distribution de vidéos streaming ... 838
Diffusez une vidéo en utilisant AWS Elemental MediaStore comme origine ... 839
Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage ... 840

Diffusez du contenu vidéo à la demande avec AWS Elemental MediaPackage 846
Résilience tenant compte de la qualité média 852
Champs de journal MQAR 855
Utilisez des fonctions pour personnaliser en périphérie 856
Différences entre CloudFront Functions et Lambda @Edge 857
Personnalisez avec des CloudFront fonctions 860
Tutoriel : Création d'une CloudFront fonction simple 861
Tutoriel : Création d'une CloudFront fonction utilisant des valeurs clés 864
Écriture du code de la fonction 867
Création de fonctions 972
Fonctions de test 976
Mise à jour de fonctions 981
Publication de fonctions 984
Association de fonctions à des distributions 985
CloudFront KeyValueStore 989
Personnalisez avec les fonctions CloudFront de connexion 1012
Vue d'ensemble et flux de travail 1013
Configuration et limites 1015
Création de fonctions de CloudFront connexion pour une validation mutuelle du protocole TLS (afficheur) 1016
Écrire le code de la fonction de CloudFront connexion pour la validation mutuelle du protocole TLS (afficheur) 1020
Testez les fonctions de CloudFront connexion avant le déploiement 1030
Associer les fonctions de connexion aux distributions 1032
Implémentez la révocation des certificats pour le TLS mutuel (visualiseur) avec CloudFront Functions et KeyValueStore 1033
Personnalisation avec Lambda@Edge 1040
Fonctionnement de Lambda@Edge avec les demandes et les réponses 1041
Comment utiliser Lambda@Edge 1042
Mise en route de Lambda@Edge 1043
Définition des rôles et autorisations IAM 1051
Écriture et création d’une fonction Lambda@Edge 1058
Ajout de déclencheurs pour une fonction Lambda@Edge 1064
Test et débogage 1071
Suppression de fonctions et de réplicas 1079
Structure d’évènements 1080

Utilisation des demandes et des réponses 1098
Exemples de fonctions 1104
Restrictions sur les fonctions périphériques 1144
Restrictions sur toutes les fonctions périphériques 1144
Restrictions relatives aux CloudFront fonctions 1151
Restrictions sur Lambda@Edge 1153
Rapports, métriques et journaux 1158
AWS rapports de facturation et d'utilisation pour CloudFront 1158
Consultez le AWS rapport de facturation pour CloudFront 1159
Consultez le AWS rapport d'utilisation pour CloudFront 1160
Interprétez votre AWS rapports de facturation et d'utilisation pour CloudFront 1162
Afficher les rapports de CloudFront console 1170
Afficher les rapports statistiques du CloudFront cache 1171
Afficher les rapports sur les objets CloudFront populaires 1177
Afficher les rapports sur CloudFront les meilleurs référents 1183
Afficher les rapports CloudFront d'utilisation 1187
Afficher les rapports des CloudFront spectateurs 1196
Surveillez CloudFront les métriques avec Amazon CloudWatch 1208
Indicateurs CloudFront des fonctions d'affichage et de périphérie 1209
Création d'alarmes 1217
Téléchargement des données de métriques 1218
CloudFront métriques 1221
CloudFront et journalisation des fonctions Edge 1228
Demandes d'enregistrement 1228
Journalisation des fonctions de périphérie 1230
Activité de service de journalisation 1230
Journaux d'accès (journaux standard) 1230
Utiliser des journaux d'accès en temps réel 1280
Journaux des fonctions de périphérie 1304
AWS CloudTrail journaux 1308
Suivez les modifications de configuration avec AWS Config 1321
Configurez AWS Config avec CloudFront 1322
Afficher l'historique CloudFront de configuration 1323
Évaluer les CloudFront configurations à l'aide de AWS Config règles 1324
Sécurité 1325
Protection des données 1326

Chiffrement en transit ... 1328
Chiffrement au repos ... 1328
Restreindre l'accès au contenu ... 1329
Gestion de l’identité et des accès ... 1330
Public ciblé ... 1330
Authentification par des identités ... 1331
Gestion de l’accès à l’aide de politiques ... 1332
Comment Amazon CloudFront travaille avec IAM ... 1334
Identity-based exemples de politiques ... 1340
AWS politiques gérées ... 1351
Utilisation de rôles liés à un service ... 1361
Résoudre les problèmes d' CloudFront identité et d'accès ... 1366
Journalisation et surveillance ... 1368
Validation de conformité ... 1369
CloudFront meilleures pratiques en matière de conformité ... 1370
Résilience ... 1372
Basculement d'origine CloudFront ... 1372
Sécurité de l’infrastructure ... 1372
Résolution des problèmes ... 1374
Résolution des problèmes de distribution ... 1374
CloudFront renvoie un Accès refusé error ... 1374
CloudFront renvoie un InvalidViewerCertificate erreur lorsque j'essaie d'ajouter un autre nom de domaine ... 1377
CloudFront renvoie une erreur d'enregistrement DNS mal configurée lorsque j'essaie d'ajouter un nouveau CNAME ... 1378
Je ne peux pas afficher les fichiers de ma distribution ... 1379
Message d'erreur : < Certificat : l'identifiant du certificat > est utilisé par CloudFront ... 1381
Résolution des problèmes liés aux codes d’état des réponses aux·erreurs ... 1381
Code d’état HTTP 400 (Requête incorrecte) ... 1382
Code d’état HTTP 401 (Accès non autorisé) ... 1383
Code d’état HTTP 403 (méthode non valide) ... 1384
Code d’état HTTP 403 (Autorisation refusée) ... 1385
Code d’état HTTP 404 (Introuvable) ... 1387
Code d’état HTTP 412 (échec de condition préalable) ... 1388
Code d’état HTTP 500 (Erreur de serveur interne) ... 1388
Code d’état HTTP 502 (Passerelle incorrecte) ... 1389

Code d'état HTTP 503 (Service non disponible) 1394
Code d'état HTTP 504 (Délai d'attente de passerelle expiré) 1397
Test de charge CloudFront 1403
Quotas 1404
Quotas généraux 1405
Quotas généraux sur les distributions 1406
Quotas généraux sur les politiques 1409
Quotas sur les MTL et les trust stores 1411
Quotas relatifs aux CloudFront fonctions 1411
Quotas relatifs aux fonctions de connexion 1412
Quotas sur les magasins de clés-valeurs 1413
Quotas sur Lambda@Edge 1413
Quotas sur les certificats SSL 1416
Quotas sur les invalidations 1416
Quotas sur les groupes clés 1417
Quotas sur WebSocket les connexions 1418
Quotas sur le chiffrement au niveau du champ 1418
Quotas sur les cookies (paramètres de cache hérités) 1419
Quotas sur les chaînes de requêtes (paramètres de cache hérités) 1419
Quotas sur les en-têtes 1420
Quotas sur les distributions multi-locataires 1421
Informations connexes 1423
Exemples de code 1424
Principes de base 1425
Actions 1426
Scénarios 1496
Création d'une distribution à locataires multiples et d'un locataire de distribution 1497
Suppression des ressources de signature 1508
Commencez avec un réseau de distribution de contenu de base 1510
Commencer à utiliser les pare-feux pour applications Web 1521
Signature des URL et des cookies 1533
CloudFront Exemples de fonctions 1537
Ajout d'en-têtes de sécurité HTTP 1538
Ajout d'un en-tête CORS 1539
Ajout d'un en-tête de contrôle de cache 1540
Ajout d'un en-tête d'adresse IP réelle du client 1541

Ajout d'un en-tête d'origine 1541
Ajout d'index.html aux URL de demande 1542
Normalisation des paramètres de chaîne de requête 1543
Redirection vers une nouvelle URL 1544
Réécriture d'une URI de demande 1546
Sélection d'une origine plus proche de l'utilisateur 1548
Utilisation de paires clé-valeur 1550
Validation d'un jeton simple 1551
Historique du document 1556
..... mdlxxxix

Qu'est-ce qu'Amazon CloudFront ?

Amazon CloudFront est un service Web qui accélère la distribution de votre contenu Web statique et dynamique, tel que les fichiers .html, .css, .js et image, à vos utilisateurs. CloudFront diffuse votre contenu via un réseau mondial de centres de données appelés emplacements périphériques. Lorsqu'un utilisateur demande du contenu que vous diffusez CloudFront, la demande est acheminée vers l'emplacement périphérique qui offre la plus faible latence (délai), afin que le contenu soit diffusé avec les meilleures performances possibles.

- Si le contenu se trouve déjà dans la zone périphérique avec la latence la plus faible, CloudFront diffusez-le immédiatement.
- Si le contenu ne se trouve pas dans cet emplacement périphérique, CloudFront récupérez-le à partir d'une origine que vous avez définie, telle qu'un compartiment Amazon S3, une MediaPackage chaîne ou un serveur HTTP (par exemple, un serveur Web) que vous avez identifié comme source de la version définitive de votre contenu.

Par exemple, supposons que vous diffusez une image à partir d'un serveur web traditionnel, et non pas à partir de CloudFront. Par exemple, vous pouvez diffuser une image, sunsetphoto.png, à l'aide de l'URL `https://example.com/sunsetphoto.png`.

Vos utilisateurs peuvent facilement accéder à cette URL et voir l'image. Néanmoins, jusqu'à ce que l'image soit trouvée, ils ignorent probablement que leur demande a été transmise d'un réseau à un autre par le biais de l'enchevêtrement complexe de réseaux interconnectés qui forment Internet.

CloudFront accélère la distribution de votre contenu en acheminant chaque demande utilisateur via le AWS réseau principal vers l'emplacement périphérique le mieux adapté à votre contenu. En règle générale, il s'agit d'un serveur de CloudFront périphérie qui fournit la diffusion la plus rapide au spectateur. L'utilisation du AWS réseau réduit considérablement le nombre de réseaux par lesquels les demandes de vos utilisateurs doivent transiter, ce qui améliore les performances. Les utilisateurs bénéficient d'une latence plus faible (durée nécessaire au chargement du premier octet du fichier) et de débits de transfert des données plus élevés.

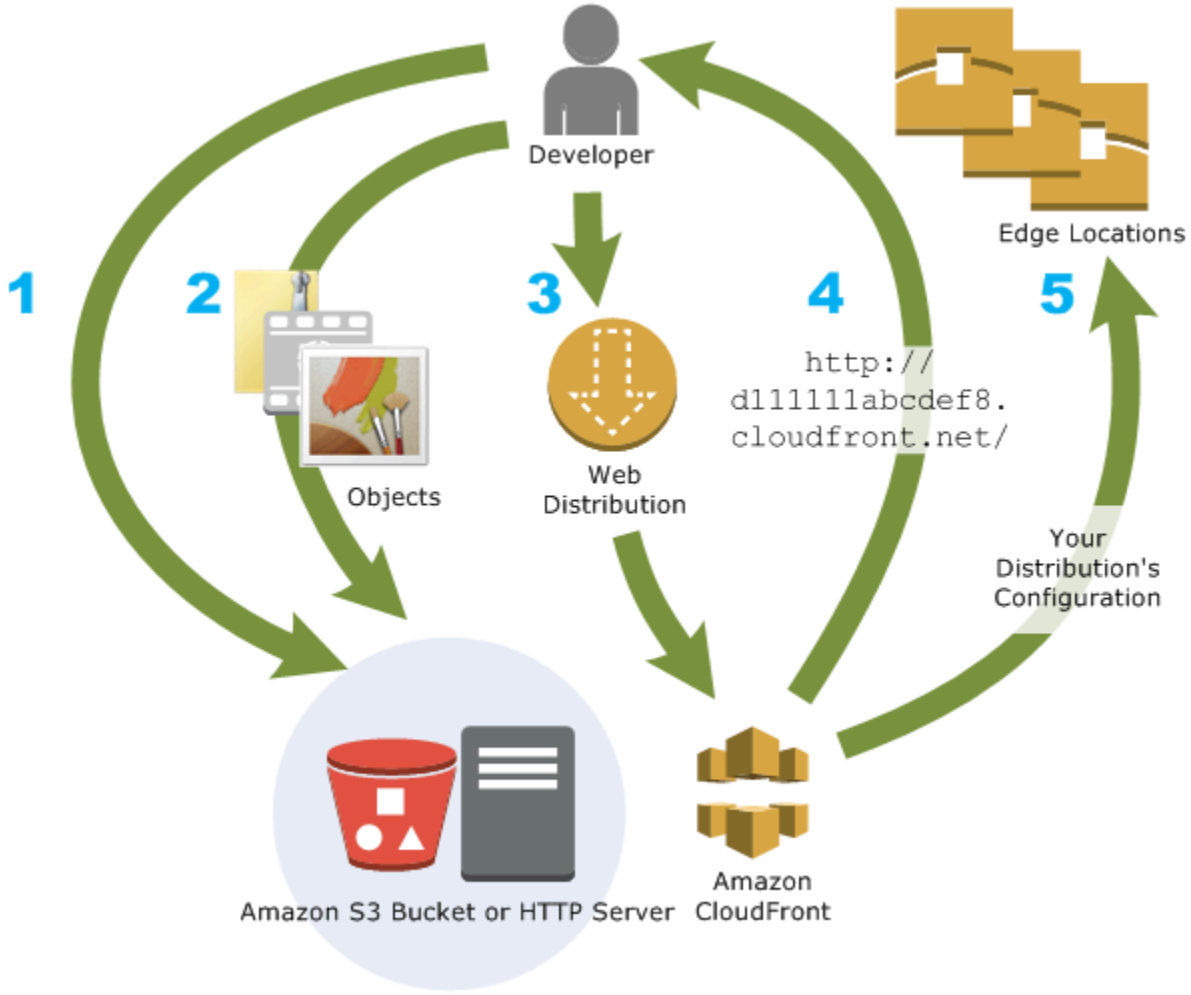
Il en résulte également une fiabilité et une disponibilité accrues, car des copies des fichiers (également appelés objets) sont désormais détenues (ou mises en cache) dans plusieurs emplacements périphériques situés aux quatre coins du monde.

Rubriques

- Comment vous configurez-vous CloudFront pour diffuser du contenu
- Choix entre une distribution standard ou une distribution multi-locataires
- Tarification
- Façons d'utiliser CloudFront
- Comment CloudFront diffuse le contenu
- Emplacements et plages d'adresses IP des serveurs CloudFront Edge
- Utilisation CloudFront avec un AWS Kit SDK
- CloudFront ressources techniques

Comment vous configurez-vous CloudFront pour diffuser du contenu

Vous créez une CloudFront distribution pour indiquer d' CloudFront où vous souhaitez que le contenu soit diffusé et pour fournir des informations détaillées sur la manière de suivre et de gérer la diffusion du contenu. CloudFront Utilise ensuite des ordinateurs (des serveurs périphériques) situés à proximité de vos spectateurs pour diffuser rapidement ce contenu lorsque quelqu'un souhaite le voir ou l'utiliser.



Comment vous configurez CloudFront pour diffuser votre contenu

1. Vous spécifiez des serveurs d'origine, tels qu'un compartiment Amazon S3 ou votre propre serveur HTTP, à CloudFront partir desquels sont extraits vos fichiers qui seront ensuite distribués depuis des emplacements CloudFront périphériques dans le monde entier.

   Un serveur d'origine stocke la version d'origine définitive de vos objets. Si vous diffusez du contenu sur HTTP, votre serveur d'origine est soit un compartiment Amazon S3 soit un serveur HTTP, tel qu'un serveur web. Votre serveur HTTP peut s'exécuter sur une instance Amazon Elastic Compute Cloud (Amazon EC2) ou sur un serveur que vous gérez ; ces serveurs sont également appelés origines personnalisées.
2. Téléchargez vos fichiers sur vos serveurs d'origine. Vos fichiers, également appelés objets, incluent généralement des pages web, des images et des fichiers multimédias, mais peuvent être tout ce qui peut être servi via HTTP.

Si vous utilisez un compartiment Amazon S3 comme serveur d'origine, vous pouvez rendre les objets de votre compartiment lisibles publiquement, afin que toute personne connaissant les CloudFront URL de vos objets puisse y accéder. Vous avez également la possibilité de garder des objets privés et de contrôler leur accès. Consultez Offre de contenu privé avec des URL et des cookies signés.

3. Vous créez une CloudFront distribution qui indique à CloudFront quels serveurs d'origine obtenir vos fichiers lorsque les utilisateurs les demandent via votre site Web ou votre application. Dans le même temps, vous spécifiez des détails tels que si vous CloudFront souhaitez enregistrer toutes les demandes et si vous souhaitez que la distribution soit activée dès sa création.
4. CloudFront attribue à votre nouvelle distribution un nom de domaine que vous pouvez voir dans la CloudFront console ou qui est renvoyé dans la réponse à une demande programmatique, par exemple une demande d'API. Si vous le souhaitez, vous pouvez ajouter un nom de domaine alternatif en remplacement.
5. CloudFront envoie la configuration de votre distribution (mais pas votre contenu) à tous ses emplacements périphériques ou points de présence (POP), c'est-à-dire des ensembles de serveurs situés dans des centres de données géographiquement dispersés où des copies de vos fichiers sont mises en CloudFront cache.

Lorsque vous développez votre site Web ou votre application, vous utilisez le nom de domaine qui CloudFront fournit vos URL. Par exemple, si CloudFront renvoie `d111111abcdef8.cloudfront.net` comme nom de domaine pour votre distribution, l'URL de logo.jpg dans votre compartiment Amazon S3 (ou dans le répertoire racine d'un serveur HTTP) est`https://d111111abcdef8.cloudfront.net/logo.jpg`.

Vous pouvez également configurer CloudFront l'utilisation de votre propre nom de domaine avec votre distribution. Dans ce cas, l'URL pourrait être `https://www.example.com/logo.jpg`.

Vous pouvez éventuellement configurer votre serveur d'origine pour ajouter des en-têtes aux fichiers, afin d'indiquer la durée pendant laquelle vous souhaitez que les fichiers restent dans le cache dans des emplacements CloudFront périphériques. Par défaut, chaque fichier reste 24 heures dans l'emplacement périphérique avant d'arriver à expiration. Le délai d'expiration minimum est de 0 seconde. Il n'existe pas de délai d'expiration maximum. Pour plus d’informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Choix entre une distribution standard ou une distribution multi-locataires

CloudFront propose des options de distribution pour des sites Web ou des applications uniques, ainsi que pour des scénarios multi-locataires.

Distribution standard

Conçue pour des configurations uniques par site web ou application. Choisissez cette option dans les cas d'utilisation suivants :

- Vous avez besoin d'une CloudFront distribution autonome
- Chaque site ou application nécessite ses propres paramètres personnalisés

La plupart des utilisateurs commencent avec une distribution standard.

Multi-tenant locataires de distribution et de distribution (CloudFront SaaS Manager)

Conçus spécifiquement pour les fournisseurs de SaaS et les scénarios multi-locataires. Choisissez cette option dans les cas d'utilisation suivants :

- Vous créez une plateforme SaaS pour desservir les sites web ou les applications de plusieurs clients
- Vous devez gérer efficacement plusieurs distributions similaires
- Vous souhaitez un contrôle centralisé des configurations partagées

Pour plus d'informations, consultez Compréhension du fonctionnement des distributions multi-locataires.

Tarification

CloudFront facture les transferts de données depuis ses emplacements périphériques, ainsi que les requêtes HTTP ou HTTPS. Les prix varient en fonction du type d'utilisation, de la région géographique et de la sélection de fonctionnalités.

Le transfert de données depuis votre point d'origine vers CloudFront est toujours gratuit lorsque vous utilisez des sites d' AWS origine tels qu'Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing ou Amazon API Gateway. Lorsque vous utilisez AWS Origins, vous n'êtes facturé que pour le transfert de données sortantes depuis et CloudFront vers le visualiseur.

Pour plus d'informations, consultez la rubrique CloudFront Tarification et FAQ sur les offres groupées de facturation et d'épargne.

Façons d'utiliser CloudFront

L'utilisation CloudFront peut vous aider à atteindre divers objectifs. Cette section en répertorie quelques-uns, avec des liens vers des informations supplémentaires, pour vous donner une idée des possibilités.

Rubriques

- Accélération de la diffusion de contenu de site web statique
- Diffusion de vidéo en streaming à la demande et en direct
- Chiffrement de champs spécifiques tout au long du traitement du système
- Personnalisation au niveau de l'emplacement périphérique
- Diffusion de contenu privé à l'aide des personnalisations de Lambda@Edge

Accélération de la diffusion de contenu de site web statique

CloudFront peut accélérer la diffusion de votre contenu statique (par exemple, des images, des feuilles de style JavaScript, etc.) aux spectateurs du monde entier. En utilisant CloudFront, vous pouvez tirer parti du réseau AWS dorsal et des serveurs de CloudFront périphérie pour offrir à vos visiteurs une expérience rapide, sûre et fiable lorsqu'ils visitent votre site Web.

Une approche simple pour stocker et diffuser du contenu statique consiste à utiliser un compartiment Amazon S3. L'utilisation conjointe de S3 CloudFront présente de nombreux avantages, notamment la possibilité d'utiliser le contrôle d'accès d'origine pour restreindre facilement l'accès à votre contenu Amazon S3.

Pour plus d'informations sur l'utilisation conjointe d'Amazon S3 CloudFront, y compris un CloudFormation modèle pour vous aider à démarrer rapidement, consultezMise en route avec un site web statique sécurisé.

Diffusion de vidéo en streaming à la demande et en direct

CloudFront propose plusieurs options pour diffuser vos contenus multimédia à des spectateurs du monde entier, qu'il s'agisse de fichiers préenregistrés ou d'événements en direct.

- Pour la diffusion de vidéos à la demande (VOD), vous pouvez CloudFront utiliser des formats courants tels que MPEG DASH, Apple HLS, Microsoft Smooth Streaming et CMAF, sur n'importe quel appareil.
- Pour diffuser du streaming en direct, vous pouvez mettre en cache des fragments multimédia à l'emplacement périphérique, de sorte que plusieurs requêtes pour le fichier manifeste qui diffuse les fragments dans le bon ordre puissent être combinées, afin de réduire la charge sur votre serveur d'origine.

Pour plus d'informations sur la façon de diffuser du contenu en streaming avec CloudFront, consultezVidéo à la demande et diffusion en direct avec CloudFront.

Chiffrement de champs spécifiques tout au long du traitement du système

Lorsque vous configurez HTTPS avec CloudFront, vous disposez déjà de connexions sécurisées de bout en bout avec les serveurs d'origine. Lorsque vous ajoutez du chiffrement au niveau du champ, vous pouvez protéger des données spécifiques tout au long du traitement du système en plus de la sécurité HTTPS, pour que seules certaines applications à votre origine puissent voir les données.

Pour configurer le chiffrement au niveau des champs, vous ajoutez une clé publique à CloudFront, puis vous spécifiez l'ensemble de champs que vous souhaitez chiffrer avec cette clé. Pour plus d'informations, consultez Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.

Personnalisation au niveau de l'emplacement périphérique

L'exécution de code sans serveur à l'emplacement périphérique offre un certain nombre de possibilités pour la personnalisation du contenu et de l'expérience des utilisateurs, à une latence réduite. Par exemple, vous pouvez renvoyer un message d'erreur personnalisé lorsque votre serveur d'origine est indisponible à des fins de maintenance, afin que les utilisateurs ne reçoivent pas de message d'erreur HTTP générique. Vous pouvez également utiliser une fonction qui permet d'autoriser les utilisateurs et de contrôler l'accès à votre contenu, avant CloudFront de transmettre une demande à votre source.

L'utilisation de Lambda @Edge CloudFront permet de personnaliser le contenu diffusé de différentes manièresCloudFront . Pour en savoir plus sur Lambda@Edge et découvrir comment créer et déployer des fonctions avec CloudFront, consultez Personnalisation en périphérie avec Lambda@Edge. Pour voir un certain nombre d'exemples de code que vous pouvez personnaliser pour vos propres solutions, consultez Exemples de fonctions Lambda@Edge.

Diffusion de contenu privé à l'aide des personnalisations de Lambda@Edge

L'utilisation de Lambda @Edge peut vous aider à configurer votre CloudFront distribution pour diffuser du contenu privé provenant de votre propre origine personnalisée, en plus d'utiliser des URL signées ou des cookies signés.

Pour diffuser du contenu privé à l'aide de CloudFront, procédez comme suit :

- Exigez des utilisateurs qu'ils accèdent au contenu à l'aide d'URL signées ou de cookies signés.
- Restreignez l'accès à votre origine afin qu'il ne soit disponible que sur les serveurs CloudFront orientés vers l'origine. Pour ce faire, vous pouvez procéder de différentes manières :
  - Pour une origine Amazon S3, vous pouvez utiliser un contrôle d'accès à l'origine (OAC).
  - Pour une origine personnalisée, vous pouvez effectuer les opérations suivantes :
    - Si l'origine personnalisée est protégée par un groupe de sécurité Amazon VPC AWS Firewall Manager, vous pouvez utiliser la liste de préfixes CloudFront gérée pour autoriser le trafic entrant vers votre origine uniquement CloudFront à partir d'adresses IP orientées vers l'origine.
    - Utilisez un en-tête HTTP personnalisé pour restreindre l'accès aux seules demandes provenant de CloudFront. Pour plus d'informations, consultez the section called "Restriction de l'accès à des fichiers d'origines personnalisées" et the section called "Ajout d'en-têtes personnalisés aux demandes d'origine". Pour voir un exemple dans lequel un en-tête personnalisé limitant l'accès à une origine Application Load Balancer est utilisé, consultez the section called "Restriction de l'accès aux Application Load Balancers".
    - Si l'origine personnalisée nécessite une logique de contrôle d'accès personnalisée, vous pouvez utiliser Lambda @Edge pour implémenter cette logique, comme décrit dans cet article de blog : Serving Private Content Using Amazon CloudFront & Lambda @Edge.

Comment CloudFront diffuse le contenu

Après quelques étapes de configuration initiale, CloudFront fonctionne avec votre site Web ou votre application et accélère la diffusion de votre contenu. Cette section explique comment votre CloudFront contenu est diffusé lorsque les internautes le demandent.

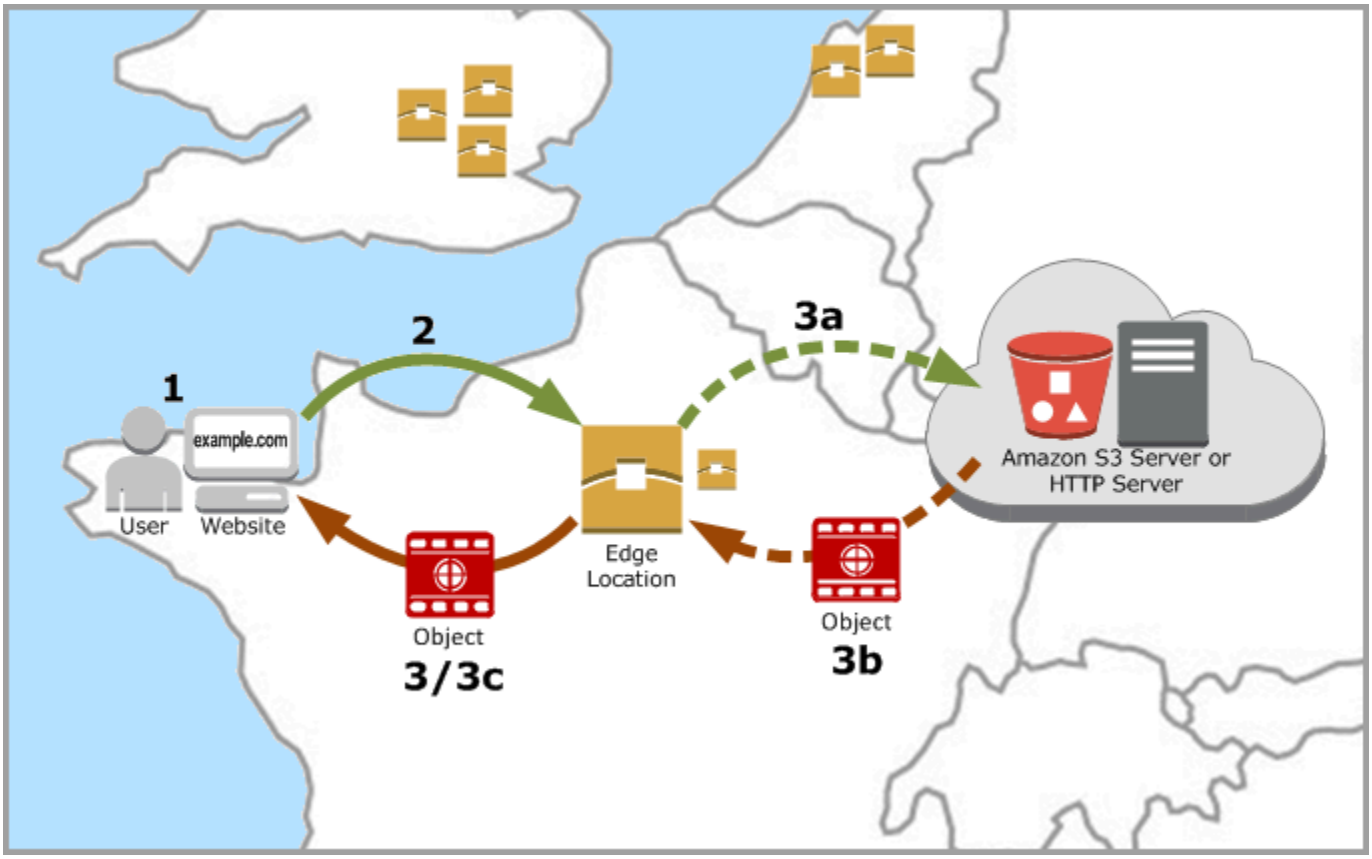
Rubriques

- Comment CloudFront diffuser du contenu à vos utilisateurs
- Comment CloudFront fonctionne avec les caches périphériques régionaux

Comment CloudFront diffuser du contenu à vos utilisateurs

Une fois que vous avez configuré CloudFront la diffusion de votre contenu, voici ce qui se passe lorsque les utilisateurs demandent vos objets :

1. Un utilisateur accède à votre application ou à votre site Web et envoie une demande pour un objet, tel qu'un fichier d'image ou un fichier HTML.
2. Le DNS achemine la demande vers le CloudFront POP (emplacement périphérique) qui peut le mieux répondre à la demande, généralement le CloudFront POP le plus proche en termes de latence.
3. CloudFront vérifie son cache pour l'objet demandé. Si l'objet se trouve dans le cache, le CloudFront renvoie à l'utilisateur. Si l'objet ne se trouve pas dans le cache, CloudFront procédez comme suit :
   a. CloudFront compare la demande aux spécifications de votre distribution et la transmet à votre serveur d'origine pour l'objet correspondant, par exemple à votre compartiment Amazon S3 ou à votre serveur HTTP.
   b. Le serveur d'origine renvoie l’objet vers l'emplacement périphérique.
   c. Dès que le premier octet arrive de l'origine, CloudFront commence à transmettre l'objet à l'utilisateur. CloudFront ajoute également l'objet au cache pour la prochaine fois que quelqu'un le demandera.



Comment CloudFront fonctionne avec les caches périphériques régionaux

CloudFront les points de présence (également appelés POPs ou emplacements périphériques) garantissent que le contenu populaire peut être diffusé rapidement à vos spectateurs. CloudFront dispose également de caches périphériques régionaux qui permettent de rapprocher une plus grande partie de votre contenu de vos spectateurs, même lorsque le contenu n'est pas assez populaire pour rester en POP, afin d'améliorer les performances de ce contenu.

Les caches périphériques régionaux aident tous les types de contenu, notamment ceux ayant tendance à devenir moins populaires au fil du temps. Il peut par exemple s'agir de contenus générés par l'utilisateur, tels que des vidéos, des photos ou des graphiques ; de ressources d’e-commerce telles que des photos et des vidéos de produits ; et de contenus liés à l'actualité et à des événements qui bénéficieraient tout à coup d'un regain de popularité.

Fonctionnement des caches régionaux

Les caches périphériques régionaux sont CloudFront des emplacements déployés dans le monde entier, à proximité de vos spectateurs. Ils sont situés entre votre serveur d'origine et les POP (ces emplacements périphériques mondiaux qui diffusent du contenu directement à vos utilisateurs). À

mesure que la popularité des objets diminue, des POP individuels peuvent supprimer ces objets pour céder la place à du contenu plus populaire. Les caches périphériques régionaux disposent d'un plus grand cache qu'un POP individuel, afin que les objets restent plus longtemps dans le cache au niveau de l'emplacement de cache périphérique régional le plus proche. Cela permet de rapprocher une plus grande partie de votre contenu de vos spectateurs, de réduire le besoin de CloudFront revenir sur votre serveur d'origine et d'améliorer les performances globales pour les spectateurs.

Lorsqu'un utilisateur effectue une demande sur votre site web ou via votre application, le DNS l'achemine vers le POP qui saura diffuser au mieux la demande de l'utilisateur. Cet emplacement est généralement l'emplacement CloudFront périphérique le plus proche en termes de latence. Dans le POP, CloudFront vérifie la présence de l'objet demandé dans son cache. Si l'objet se trouve dans le cache, le CloudFront renvoie à l'utilisateur. S'il n'est pas dans le cache, le POP accède au cache périphérique régional le plus proche pour l'extraire. Pour plus d'informations sur le moment où le POP ignore le cache périphéruqe régional et accède directement à l'origine, reportez-vous à la note suivante.

Dans l'emplacement du cache périphérique régional, vérifie CloudFront à nouveau son cache pour l'objet demandé. Si l'objet se trouve dans le cache, le CloudFront transmet au POP qui l'a demandé. Dès que le premier octet arrive depuis l'emplacement du cache périphérique régional, l'objet CloudFront commence à être transféré à l'utilisateur. CloudFront ajoute également l'objet au cache du POP pour la prochaine fois que quelqu'un en fera la demande.

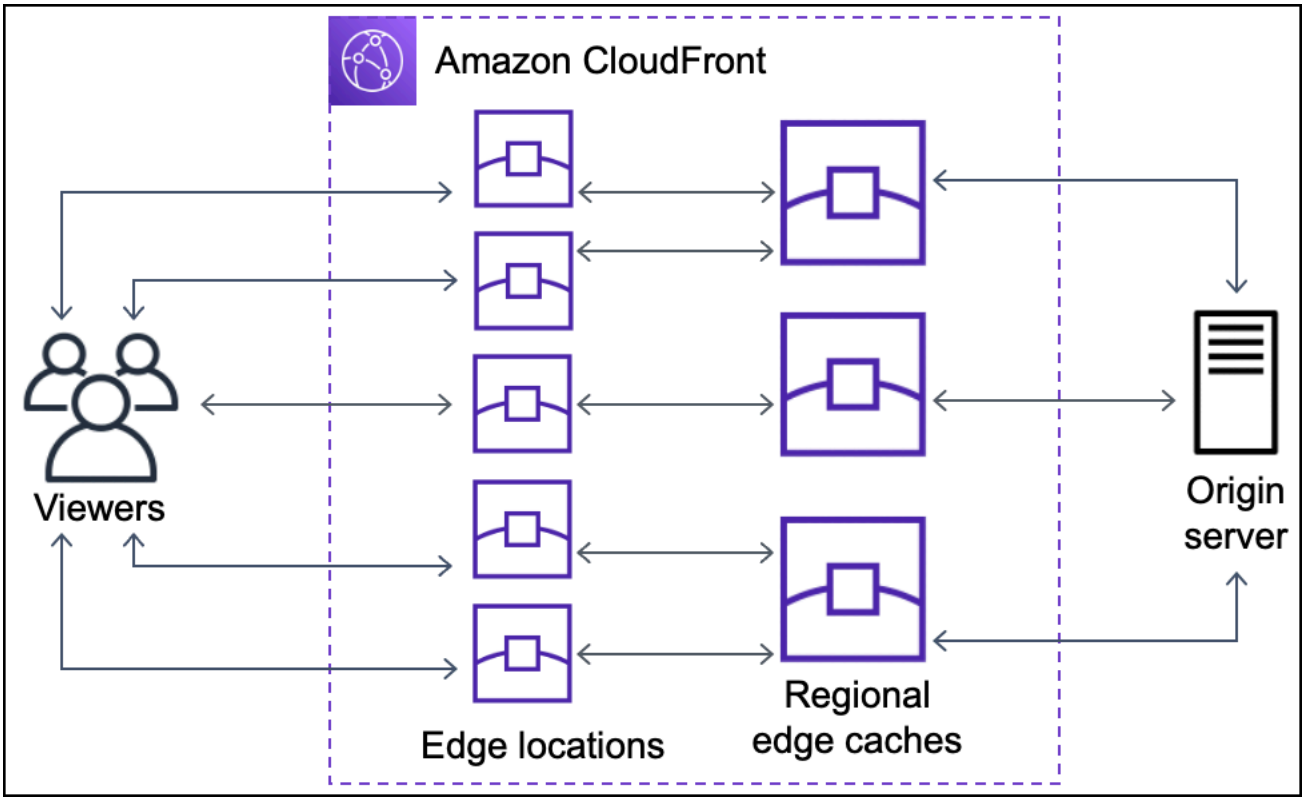
Pour les objets qui ne sont pas mis en cache au point POP ou à l'emplacement du cache périphérique régional, CloudFront compare la demande aux spécifications de vos distributions et transmet la demande au serveur d'origine. Une fois que votre serveur d'origine a renvoyé l'objet à l'emplacement du cache périphérique régional, il est transféré au POP CloudFront , puis à l'utilisateur. Dans ce cas, ajoute CloudFront également l'objet au cache situé à l'emplacement du cache périphérique régional en plus du POP pour la prochaine fois qu'un utilisateur le demandera. Cela garantit que tous les POP d'une région partagent un cache local, éliminant ainsi les demandes multiples adressées aux serveurs d'origine. CloudFront conserve également des connexions persistantes avec les serveurs d'origine afin que les objets soient récupérés depuis les sources le plus rapidement possible.

> **Note**
>
> - Les caches périphériques régionaux présentent une parité de fonctionnalités avec les POP. Par exemple, une demande d'invalidation d'un cache supprime un objet à la fois des caches des POP et des caches périphériques régionaux avant son expiration. La prochaine

fois qu'un utilisateur demande l'objet, CloudFront revient à l'origine pour extraire la dernière version de l'objet.

- Les méthodes proxy HTTP (`PUT`, `POST`, `PATCH`, `OPTIONS` et `DELETE`) se dirigent directement vers l'origine depuis les POP sans passer par les caches périphériques régionaux.
- Les demandes dynamiques, tel que déterminé au moment de la demande, ne circulent pas dans les caches périphériques régionaux, mais vont directement à l'origine.
- Lorsque l'origine est un compartiment Amazon S3 et que le cache périphérique régional optimal de la demande se trouve dans le même compartiment Région AWS que le compartiment S3, le POP ignore le cache périphérique régional et passe directement au compartiment S3.

Le schéma suivant illustre la façon dont les demandes et les réponses circulent dans les emplacements CloudFront périphériques et les caches périphériques régionaux.



Emplacements et plages d'adresses IP des serveurs CloudFront Edge

Pour obtenir la liste des emplacements des serveurs CloudFront Edge, consultez la page Amazon CloudFront Global Edge Network.

Amazon Web Services (AWS) publie ses plages d'adresses IP actuelles au format JSON. Pour afficher les plages actuelles, téléchargez ip-ranges.json. Pour plus d'informations, consultez Plages d'adresses IP AWS dans le Référence générale d'Amazon Web Services.

Pour trouver les plages d'adresses IP associées aux serveurs CloudFront Edge, recherchez la chaîne suivante sur ip-ranges.json :

```
"region": "GLOBAL",
"service": "CLOUDFRONT"
```

Vous pouvez également afficher uniquement les plages CloudFront IP àhttps://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips.

Utiliser la liste de préfixes CloudFront gérée

La liste des préfixes CloudFront gérés contient les plages d'adresses IP de tous les serveurs orientés vers l'origine distribués CloudFront dans le monde entier. Si votre origine est hébergée AWS et protégée par un groupe de sécurité Amazon VPC, vous pouvez utiliser la liste de CloudFront préfixes gérée. La liste des préfixes autorise le trafic entrant vers votre point d'origine uniquement en provenance de serveurs CloudFront orientés vers l'origine, ce qui empêche le trafic autre que le CloudFront trafic d'atteindre votre origine. CloudFront gère la liste des préfixes gérés afin qu'elle soit toujours à jour avec les adresses IP de tous les serveurs CloudFront mondiaux orientés vers l'origine. Avec la liste de préfixes CloudFront gérée, vous n'avez pas besoin de lire ou de gérer vous-même une liste de plages d'adresses IP.

Par exemple, imaginez que votre origine soit une instance Amazon EC2 située dans la région Europe (Londres) (`eu-west-2`). Si l'instance se trouve dans un VPC, vous pouvez créer une règle de groupe de sécurité qui autorise l'accès HTTPS entrant à partir de la liste des CloudFront préfixes gérés. Cela permet à tous les serveurs CloudFront mondiaux orientés vers l'origine d'accéder à l'instance. Si vous supprimez toutes les autres règles entrantes du groupe de sécurité, vous empêchez tout trafic autre que le CloudFront trafic d'atteindre l'instance.

Les listes de préfixes CloudFront gérées sont les suivantes :

- `com.amazonaws.global.cloudfront.origin-facing` (IPv4)
- `com.amazonaws.global.ipv6.cloudfront.origin-facing` (IPv6)

Pour plus d'informations, consultez la section Utiliser une liste de préfixes AWS gérée dans le guide de l'utilisateur Amazon VPC.

> **Important**
>
> La liste de préfixes CloudFront gérés est unique en ce sens qu'elle s'applique aux quotas Amazon VPC. Pour plus d'informations, consultez la pondération de la liste de préfixes gérés par AWS dans le Guide de l'utilisateur Amazon VPC.

Utilisation CloudFront avec un AWS Kit SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation courants. Chaque kit SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK pour C++	AWS SDK pour C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK pour Go	AWS SDK pour Go exemples de code
AWS SDK pour Java	AWS SDK pour Java exemples de code
AWS SDK pour JavaScript	AWS SDK pour JavaScript exemples de code
AWS SDK pour Kotlin	AWS SDK pour Kotlin exemples de code
AWS SDK pour .NET	AWS SDK pour .NET exemples de code
AWS SDK pour PHP	AWS SDK pour PHP exemples de code
Outils AWS pour PowerShell	Outils AWS pour PowerShell exemples de code

Documentation SDK	Exemples de code
AWS SDK pour Python v4	AWS Exemples de code du SDK pour Python v4
AWS SDK pour Python (Boto3)	AWS SDK pour Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code
AWS SDK pour Rust	AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
AWS SDK pour Swift	AWS SDK pour Swift exemples de code

Exemple de disponibilité

Vous n'avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Faire un commentaire en bas de cette page.

CloudFront ressources techniques

Utilisez les ressources suivantes pour obtenir des réponses à des questions techniques concernant CloudFront :

- AWS Re:post — Un site communautaire de questions-réponses permettant aux développeurs de discuter de questions techniques liées à. CloudFront
- Support Centre — Ce site contient des informations sur vos demandes d'assistance récentes, les résultats et AWS Trusted Advisor les bilans de santé. Il propose aussi des liens vers les forums de discussion, les FAQ techniques, le tableau de bord de l'état des services et des informations sur les plans de Support .
- AWS Support Premium : découvrez le support AWS Premium, un canal d'assistance personnalisé et rapide qui vous aide à créer et à exécuter des applications. AWS

Commencez avec CloudFront

Les rubriques de cette section vous montrent comment commencer à diffuser votre contenu avec Amazon CloudFront.

La Configurez votre Compte AWS rubrique décrit les prérequis pour les didacticiels suivants, tels que la création d'un Compte AWS et la création d'un utilisateur doté d'un accès administratif.

Le didacticiel de distribution de base vous montre comment configurer le contrôle d'accès d'origine (OAC) pour envoyer des demandes authentifiées à une origine Amazon S3.

Le didacticiel pour site web statique sécurisé explique comment créer un site web statique sécurisé pour votre nom de domaine à l'aide d'un OAC et d'une origine Amazon S3. Le didacticiel utilise un modèle Amazon CloudFront (CloudFront) pour la configuration et le déploiement.

Le AWS CLI didacticiel explique comment créer, mettre à jour et supprimer une distribution standard à l'aide de AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez Mise en route avec une distribution standard (AWS CLI).

Rubriques

- Configurez votre Compte AWS
- Commencez avec une distribution CloudFront standard
- Mise en route avec une distribution standard (AWS CLI)
- Mise en route avec un site web statique sécurisé

Configurez votre Compte AWS

Cette rubrique décrit les étapes préliminaires, telles que la création d'un Compte AWS, pour vous préparer à utiliser Amazon CloudFront.

Rubriques

- Inscrivez-vous pour un Compte AWS
- Choisissez le mode d'accès CloudFront

Inscrivez-vous pour un Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Il existe deux façons de s'inscrire à AWS. Si vous souhaitez contrôler totalement la configuration de votre compte et l'emplacement de stockage de votre contenu, ou si vous avez des charges de travail réglementées telles que HIPAA ou FedRAMP, utilisez Sign up for (advanced). AWS Si vous êtes un nouvel utilisateur et que vous souhaitez utiliser un identifiant que vous possédez déjà pour vous connecter AWS et créer un AWS environnement avec des paramètres par défaut préconfigurés dans Select Régions AWS, utilisez S'inscrire pour. AWS

Choisissez le mode d'accès CloudFront

Vous pouvez accéder CloudFront à Amazon de différentes manières :

- Console de gestion AWS— Les procédures décrites dans ce guide expliquent comment utiliser le Console de gestion AWS pour effectuer des tâches.
- AWS SDK — Si vous utilisez un langage de programmation qui AWS fournit un SDK pour, vous pouvez utiliser un SDK pour y accéder. CloudFront Les SDK simplifient l'authentification, s'intègrent facilement à votre environnement de développement et fournissent un accès aux CloudFront commandes. Pour plus d'informations, consultez Utilisation CloudFront avec un AWS Kit SDK.
- CloudFront API — Si vous utilisez un langage de programmation pour lequel aucun SDK n'est disponible, consultez le Amazon CloudFront API Reference pour plus d'informations sur les actions d'API et sur la manière de faire des demandes d'API.
- AWS CLI— Le AWS Command Line Interface (AWS CLI) est un outil de gestion unifié Services AWS. Pour en savoir plus sur la manière d'installer et de configurer l' AWS CLI, consultez Installation ou mise à jour de la dernière version de l' AWS CLI dans le Guide de l'utilisateur de l'AWS Command Line Interface .
- Outils pour Windows PowerShell — Si vous avez de l'expérience avec Windows PowerShell, vous préférerez peut-être utiliser AWS Tools for Windows PowerShell. Pour plus d'informations, consultez Installation d' AWS Tools for Windows PowerShell dans le Guide de l'utilisateur Outils AWS pour PowerShell .

Commencez avec une distribution CloudFront standard

Les procédures décrites dans cette section vous indiquent comment CloudFront configurer une distribution standard qui effectue les opérations suivantes :

- Création d’un compartiment S3 comme origine de votre distribution.
- Stockage des versions d’origine de vos objets dans un compartiment Amazon Simple Storage Service (Amazon S3).
- Utilisation du contrôle d’accès d’origine (OAC) pour envoyer des demandes authentifiées à votre origine Amazon S3. L'OAC envoie des demandes CloudFront pour empêcher les utilisateurs d'accéder directement à votre compartiment S3. Pour plus d’informations sur l’OAC, consultez Restriction de l’accès à une origine Amazon S3.
- Utilise le nom de CloudFront domaine dans les URL de vos objets (par exemple,`https://d111111abcdef8.cloudfront.net/index.html`).
- Maintient vos objets dans des emplacements CloudFront périphériques pendant la durée par défaut de 24 heures (la durée minimale est de 0 seconde).

La plupart de ces paramètres sont configurés automatiquement pour vous lorsque vous créez une CloudFront distribution.

Rubriques

- Conditions préalables
- Créer un compartiment Amazon S3
- Chargement du contenu dans le compartiment
- Créez une CloudFront distribution qui utilise une origine Amazon S3 avec OAC
- Accédez à votre contenu via CloudFront
- Nettoyage
- Amélioration de votre distribution de base

Conditions préalables

Avant de commencer, vérifiez que vous avez bien terminé les étapes de Configurez votre Compte AWS.

Créer un compartiment Amazon S3

Un compartiment Amazon S3 est un conteneur pour des fichiers (objets) ou des dossiers. CloudFront peut distribuer presque n'importe quel type de fichier pour vous lorsqu'un compartiment S3 est la

source. Par exemple, CloudFront peut distribuer du texte, des images et des vidéos. La quantité de données que vous pouvez stocker sur Amazon S3 n'est pas limitée.

Dans ce didacticiel, vous allez créer un compartiment S3 contenant les fichiers d'exemple `hello world` fournis, que vous utiliserez pour créer une page web de base.

Pour créer un compartiment

1. Connectez-vous à la console Amazon S3 Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Nous vous recommandons d'utiliser notre exemple Hello World pour ce guide de démarrage. Téléchargez la page web Hello world : hello-world-html.zip. Décompressez-le, puis enregistrez le dossier `css` et le fichier `index` à un emplacement pratique, par exemple sur le bureau où vous utilisez votre navigateur.
3. Choisissez Créer un compartiment.
4. Entrez un Nom de compartiment unique conforme aux Règles de dénomination des compartiments à usage général du Guide de l'utilisateur Amazon Simple Storage Service.
5. Pour la Région, nous vous recommandons de choisir une Région AWS géographiquement proche de vous. (Ce choix réduit la latence et les coûts.)
   - Vous pouvez également sélectionner une autre région. Vous pourriez le faire, par exemple, pour répondre à des exigences réglementaires.
6. Conservez aux autres paramètres leurs valeurs par défaut, puis cliquez sur Créer un compartiment.

Chargement du contenu dans le compartiment

Après avoir créé votre compartiment Amazon S3, téléchargez-y le contenu du fichier `hello world` décompressé. (Vous avez téléchargé et décompressé ce fichier dans Créer un compartiment Amazon S3.)

Pour charger le contenu dans Amazon S3

1. Dans la section Compartiments à usage général, choisissez le nom de votre nouveau compartiment.
2. Choisissez Charger.
3. Sur la page Charger, faites glisser le dossier `css` et le fichier `index` jusqu'à la zone de dépôt.

4. Laissez tous les autres paramètres avec leur valeur par défaut, puis sélectionnez Charger.

Créez une CloudFront distribution qui utilise une origine Amazon S3 avec OAC

Dans le cadre de ce didacticiel, vous allez créer une CloudFront distribution qui utilise une origine Amazon S3 avec un contrôle d'accès à l'origine (OAC). L'OAC vous permet d'envoyer en toute sécurité des demandes authentifiées à votre origine Amazon S3. Pour plus d'informations sur l'OAC, consultez Restriction de l'accès à une origine Amazon S3.

Pour créer une CloudFront distribution avec une origine Amazon S3 qui utilise OAC

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Créer une distribution.
3. Entrez un Nom de distribution pour la distribution standard. Le nom sera affiché comme valeur pour la clé `Name` sous forme de balise. Cette valeur peut être modifiée par la suite. Vous pouvez ajouter jusqu'à 50 balises pour votre distribution standard. Pour plus d'informations, consultez Marquer une CloudFront ressource.
4. Choisissez Site web ou application unique, puis Suivant.
5. Choisissez Suivant.
6. Sur la page Type de l'origine, sélectionnez Amazon S3.
7. Pour Origine S3, choisissez Parcourir S3 et sélectionnez le compartiment S3 que vous avez créé pour ce didacticiel.
8. Dans Paramètres, choisissez Utiliser les paramètres d'origine recommandés. CloudFront utilisera les paramètres de cache et d'origine recommandés par défaut pour votre origine Amazon S3, y compris la configuration du contrôle d'accès à l'origine (OAC). Pour plus d'informations sur les paramètres recommandés, consultez Référence des paramètres de distribution préconfigurés.
9. Choisissez Suivant.
10. Sur la page Activer les protections de sécurité, choisissez si vous souhaitez activer les protections AWS WAF de sécurité.
11. Choisissez Suivant.
12. Choisissez Créer une distribution. CloudFront met à jour la politique relative aux compartiments S3 pour vous.

13. Examinez la section Détails de la nouvelle distribution. Lorsque le déploiement de votre distribution est terminé, le champ Dernière modification passe de Déploiement à une date et une heure.
14. Enregistrez le nom de domaine CloudFront attribué à votre distribution. Il ressemble à ce qui suit: `d111111abcdef8.cloudfront.net`.

Avant d'utiliser la distribution et le compartiment S3 décrits dans ce didacticiel dans un environnement de production, vérifiez qu'ils sont configurés pour répondre à vos besoins spécifiques. Pour en savoir plus sur la configuration de l'accès dans un environnement de production, consultez Configuration d'un accès sécurisé et restriction de l'accès au contenu.

Accédez à votre contenu via CloudFront

Pour accéder à votre contenu via CloudFront, associez le nom de domaine de votre CloudFront distribution à la page principale de votre contenu. (Vous avez enregistré votre nom de domaine de distribution dans Créez une CloudFront distribution qui utilise une origine Amazon S3 avec OAC.)

- Le nom de domaine de votre distribution se présente sous cette forme : `d111111abcdef8.cloudfront.net`.
- Le chemin de la page principale d'un site web est généralement `/index.html`.

Par conséquent, l'URL permettant d'accéder à votre contenu CloudFront peut ressembler à ceci :

`https://d111111abcdef8.cloudfront.net/index.html`.

Si vous avez suivi les étapes précédentes et utilisé la page web hello world, vous devriez voir une page web affichant Hello world!.

Lorsque vous chargez du contenu supplémentaire dans ce compartiment S3, vous pouvez y accéder en CloudFront combinant le nom de domaine de CloudFront distribution avec le chemin d'accès à l'objet dans le compartiment S3. Par exemple, si vous chargez un nouveau fichier nommé `new-page.html` à la racine de votre compartiment S3, l'URL se présente comme suit :

`https://d111111abcdef8.cloudfront.net/new-page.html`.

Nettoyage

Si vous avez créé votre distribution et votre compartiment S3 uniquement à des fins d'apprentissage, supprimez-les afin de ne plus encourir de coûts. Commencez par supprimer la distribution. Pour plus d'informations, consultez les liens suivants :

- Supprimer une distribution
- Supprimer un bucket

Amélioration de votre distribution de base

Ce didacticiel de mise en route fournit un cadre minimal pour créer une distribution. Nous vous recommandons d'explorer les améliorations suivantes :

- Vous pouvez utiliser la fonctionnalité de contenu CloudFront privé pour restreindre l'accès au contenu des compartiments Amazon S3. Pour plus d'informations sur la distribution de contenus privés, consultez Offre de contenu privé avec des URL et des cookies signés.
- Vous pouvez configurer votre CloudFront distribution pour utiliser un nom de domaine personnalisé (par exemple, `www.example.com` au lieu `ded111111abcdef8.cloudfront.net`). Pour plus d'informations, consultez Utilisation d'URL personnalisées.
- Ce didacticiel utilise une origine Amazon S3 avec un contrôle d'accès d'origine (OAC). Cependant, vous ne pouvez pas utiliser l'OAC si votre origine est un compartiment S3 configuré comme point de terminaison de site web. Si tel est le cas, vous devez configurer votre bucket en CloudFront tant qu'origine personnalisée. Pour plus d'informations, consultez Utilisation d'un compartiment Amazon S3 configuré en tant que point de terminaison de site web. Pour plus d'informations sur l'OAC, consultez Restriction de l'accès à une origine Amazon S3.

Mise en route avec une distribution standard (AWS CLI)

Les procédures décrites dans cette section vous montrent comment utiliser le AWS CLI with CloudFront pour configurer une configuration de base impliquant les éléments suivants :

- Création d'un compartiment Amazon S3 comme origine de votre distribution.
- Stockage des versions d'origine de vos objets dans le compartiment S3.
- Utilisation du contrôle d'accès d'origine (OAC) pour envoyer des demandes authentifiées à votre origine Amazon S3. L'OAC envoie des demandes CloudFront pour empêcher les utilisateurs

d'accéder directement à votre compartiment S3. Pour plus d'informations sur l'OAC, consultez Restriction de l'accès à une origine Amazon S3.

- Utiliser le nom de CloudFront domaine URLs pour vos objets (par exemple,`https://d111111abcdef8.cloudfront.net/index.html`).
- Conserver vos objets dans des emplacements CloudFront périphériques pendant la durée par défaut de 24 heures (la durée minimale est de 0 seconde).

La plupart de ces options sont personnalisables. Pour plus d'informations sur la personnalisation de vos options de distribution CloudFront consultez Créer une distribution.

Conditions préalables

Avant de commencer, vérifiez que vous avez bien terminé les étapes de Configurez votre Compte AWS.

Installez-le AWS CLI et configurez-le avec vos informations d'identification. Pour plus d'informations, consultez Mise en route avec le AWS CLI dans le AWS CLI Guide de l'utilisateur.

Créer un compartiment Amazon S3

Un compartiment Amazon S3 est un conteneur pour des fichiers (objets) ou des dossiers. CloudFront peut distribuer presque n'importe quel type de fichier pour vous lorsqu'un compartiment S3 est la source. Par exemple, CloudFront peut distribuer du texte, des images et des vidéos. La quantité de données que vous pouvez stocker sur Amazon S3 n'est pas limitée.

Dans ce didacticiel, vous allez créer un compartiment S3 et télécharger un fichier HTML qui servira à générer une page web simple.

```
aws s3 mb s3://amzn-s3-demo-bucket/ --region us-east-1
```

*amzn-s3-demo-bucket*Remplacez-le par un nom de compartiment unique au monde. Pour cela Région AWS, nous vous recommandons de choisir une région géographiquement proche de vous. Cette approche diminue la latence et les coûts, bien qu'il soit tout à fait possible d'utiliser une autre région. Par exemple, vous pouvez procéder ainsi afin de satisfaire à des exigences réglementaires.

Chargement du contenu dans le compartiment

Pour ce didacticiel, téléchargez et extrayez les fichiers de contenu d'exemple pour une page web « Hello World » basique.

```
# Create a temporary directory
mkdir -p ~/cloudfront-demo

# Download the sample Hello World files
curl -o ~/cloudfront-demo/hello-world-html.zip https://docs.aws.amazon.com/
AmazonCloudFront/latest/DeveloperGuide/samples/hello-world-html.zip

# Extract the zip file
unzip ~/cloudfront-demo/hello-world-html.zip -d ~/cloudfront-demo/hello-world
```

Cette opération crée un répertoire contenant un fichier `index.html` et un dossier `css`. Chargez ces fichier dans votre compartiment S3.

```
aws s3 cp ~/cloudfront-demo/hello-world/ s3://amzn-s3-demo-bucket/ --recursive
```

Création d'un contrôle d'accès d'origine (OAC)

Dans ce didacticiel, vous allez créer un contrôle d'accès d'origine (OAC). L'OAC vous permet d'envoyer en toute sécurité des demandes authentifiées à votre origine Amazon S3. Pour plus d'informations sur l'OAC, consultez Restriction de l'accès à une origine Amazon S3.

```
aws cloudfront create-origin-access-control \
    --origin-access-control-config Name="oac-for-
s3",SigningProtocol=sigv4,SigningBehavior=always,OriginAccessControlOriginType=s3
```

Enregistrez l'ID de l'OAC fourni dans la sortie en tant que variable d'environnement. Remplacez les exemples de valeurs par votre propre ID d'OAC. Vous l'utiliserez à l'étape suivante.

```
OAC_ID="E1ABCD2EFGHIJ"
```

Création d'une distribution standard

Créez un fichier de configuration de distribution nommé `distribution-config.json`. Remplacez le nom de compartiment de l'exemple par le vôtre pour les valeurs `Id`, `DomainName` et `TargetOriginId`.

```
cat > distribution-config.json << EOF
{
    "CallerReference": "cli-example-$(date +%s)",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "S3-amzn-s3-demo-bucket",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                },
                "OriginAccessControlId": "$OAC_ID"
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "S3-amzn-s3-demo-bucket",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["GET", "HEAD"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["GET", "HEAD"]
            }
        },
        "DefaultTTL": 86400,
        "MinTTL": 0,
        "MaxTTL": 31536000,
        "Compress": true,
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            }
        }
    },
    "Comment": "CloudFront distribution for S3 bucket",
    "Enabled": true
}
EOF
```

Créez la distribution standard.

```
aws cloudfront create-distribution --distribution-config file://distribution-
config.json
```

Enregistrez l'ID de distribution et le nom de domaine de la sortie en tant que variables d'environnement. Remplacez les exemples de valeurs par les vôtres. Vous les utiliserez ultérieurement dans ce didacticiel.

```
DISTRIBUTION_ID="EABCD1234XMPL"
DOMAIN_NAME="d111111abcdef8.cloudfront.net"
```

Avant d'utiliser la distribution et le compartiment S3 décrits dans ce didacticiel dans un environnement de production, vérifiez qu'ils sont configurés pour répondre à vos besoins spécifiques. Pour en savoir plus sur la configuration de l'accès dans un environnement de production, consultez Configuration d'un accès sécurisé et restriction de l'accès au contenu.

Mise à jour de votre stratégie de compartiment S3

Mettez à jour votre politique de compartiment S3 CloudFront pour autoriser l'accès aux objets. Remplacez le nom de compartiment utilisé dans l'exemple par le nom de votre compartiment.

```
# Get your AWS account ID
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create the bucket policy
cat > bucket-policy.json << EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
```

```
                    "AWS:SourceArn": "arn:aws:cloudfront::$ACCOUNT_ID:distribution/
$DISTRIBUTION_ID"
                }
            }
        }
    ]
}
EOF

# Apply the bucket policy
aws s3api put-bucket-policy \
    --bucket amzn-s3-demo-bucket \
    --policy file://bucket-policy.json
```

Confirmation du déploiement de la distribution

Une fois votre distribution créée, le déploiement prendra un certain temps. Lorsque l'état de distribution passe de `InProgress` à `Deployed`, passez à l'étape suivante.

```
aws cloudfront get-distribution --id $DISTRIBUTION_ID --query 'Distribution.Status'
```

Vous pouvez également utiliser la commande `wait` pour attendre le déploiement de la distribution.

```
aws cloudfront wait distribution-deployed --id $DISTRIBUTION_ID
```

Accédez à votre contenu via CloudFront

Pour accéder à votre contenu via CloudFront, associez le nom de domaine de votre CloudFront distribution à la page principale de votre contenu. Remplacez l'exemple CloudFront de nom de domaine par le vôtre.

```
https://d111111abcdef8.cloudfront.net/index.html
```

Si vous avez suivi les étapes précédentes et créé le fichier HTML, vous devriez voir une page web affichant Hello world!.

Lorsque vous chargez du contenu supplémentaire dans ce compartiment S3, vous pouvez y accéder en CloudFront combinant le nom de domaine de CloudFront distribution avec le chemin d'accès à l'objet dans le compartiment S3. Par exemple, si vous chargez un nouveau fichier nommé `new-page.html` à la racine de votre compartiment S3, l'URL se présente comme suit :

`https://d111111abcdef8.cloudfront.net/new-page.html`.

Nettoyage

Si vous avez créé votre distribution et votre compartiment S3 uniquement à des fins d'apprentissage, supprimez-les afin de ne plus encourir de coûts. Commencez par désactiver et supprimer la distribution.

Pour désactiver et supprimer une distribution standard (AWS CLI)

1. Tout d'abord, désactivez la distribution.

```
# Get the current configuration and ETag
ETAG=$(aws cloudfront get-distribution-config --id $DISTRIBUTION_ID --query 'ETag'
 --output text)

# Create a modified configuration with Enabled=false
aws cloudfront get-distribution-config --id $DISTRIBUTION_ID | \
jq '.DistributionConfig.Enabled = false' > temp_disabled_config.json

# Update the distribution to disable it
aws cloudfront update-distribution \
    --id $DISTRIBUTION_ID \
    --distribution-config file://<(jq '.DistributionConfig'
 temp_disabled_config.json) \
    --if-match $ETAG
```

2. Attendez que la distribution soit désactivée.

```
aws cloudfront wait distribution-deployed --id $DISTRIBUTION_ID
```

3. Supprimez la distribution.

```
# Get the current ETag
ETAG=$(aws cloudfront get-distribution-config --id $DISTRIBUTION_ID --query 'ETag'
 --output text)

# Delete the distribution
aws cloudfront delete-distribution --id $DISTRIBUTION_ID --if-match $ETAG
```

Pour supprimer un compartiment S3 (AWS CLI)

- Supprimez le compartiment S3 et son contenu. Remplacez le nom de compartiment utilisé dans l'exemple par le vôtre.

```
# Delete the bucket contents
aws s3 rm s3://amzn-s3-demo-bucket --recursive

# Delete the bucket
aws s3 rb s3://amzn-s3-demo-bucket
```

Pour nettoyer les fichiers locaux créés pour ce didacticiel, exécutez les commandes suivantes :

```
# Clean up local files
rm -f distribution-config.json bucket-policy.json temp_disabled_config.json
rm -rf ~/cloudfront-demo
```

Vous pouvez éventuellement supprimer l'OAC que vous avez créé pour ce didacticiel.

```
# Get the OAC ETag
OAC_ETAG=$(aws cloudfront get-origin-access-control --id $OAC_ID --query 'ETag' --
output text)

# Delete the OAC
aws cloudfront delete-origin-access-control --id $OAC_ID --if-match $OAC_ETAG
```

Mise en route avec un site web statique sécurisé

Vous pouvez commencer à utiliser Amazon CloudFront en utilisant la solution décrite dans cette rubrique pour créer un site Web statique sécurisé pour votre nom de domaine. Un site Web statique utilise uniquement des fichiers statiques, tels que du HTML, du CSS, JavaScript des images et des vidéos, et n'a pas besoin de serveurs ou de traitement côté serveur. Avec cette solution, votre site web bénéficie des avantages suivants :

- Utilise le stockage durable d'Amazon Simple Storage Service (Amazon S3) – Cette solution crée un compartiment Amazon S3 pour héberger le contenu de votre site web statique. Pour mettre à jour votre site web, il vous suffit de charger vos nouveaux fichiers dans le compartiment S3.

- Accéléré par le réseau de diffusion de CloudFront contenu Amazon — Cette solution crée une CloudFront distribution pour diffuser votre site Web aux visiteurs avec une faible latence. La distribution est configurée avec le contrôle d'accès à l'origine (OAC) pour garantir que le site Web est accessible uniquement via S3 CloudFront, et non directement depuis S3.
- Est sécurisé par HTTPS et des en-têtes de sécurité : cette solution crée un SSL/TLS certificat dans AWS Certificate Manager (ACM) et l'attache à la CloudFront distribution. Ce certificat permet à la distribution de diffuser le site web de votre domaine en toute sécurité avec HTTPS.
- Est configurée et déployée avec AWS CloudFormation: cette solution utilise un CloudFormation modèle pour configurer tous les composants, afin que vous puissiez vous concentrer davantage sur le contenu de votre site Web et moins sur la configuration des composants.

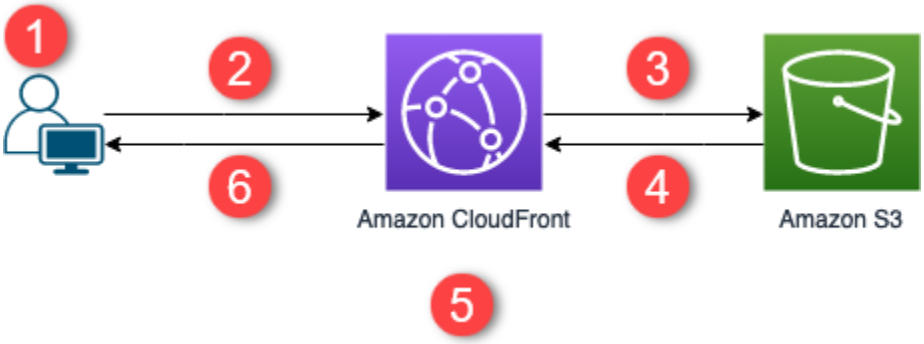
Cette solution est open source sur GitHub. Pour afficher le code, envoyer une demande d'extraction ou ouvrir un problème, accédez à https://github.com/aws-samples/amazon-cloudfront-secure-static-site.

Rubriques

- Présentation de la solution
- Déploiement de la solution

Présentation de la solution

Le diagramme suivant présente un aperçu du fonctionnement de cette solution de site web statique :



1. L'utilisateur demande le site web à l'adresse www.example.com.
2. Si l'objet demandé est mis en cache, CloudFront renvoie l'objet de son cache au visualiseur.
3. Si l'objet n'est pas dans le CloudFront cache, CloudFront demande l'objet depuis l'origine (un compartiment S3).

4. S3 renvoie l'objet à CloudFront.
5. CloudFront met en cache l'objet.
6. Les objets sont renvoyés à l’utilisateur. Les demandes suivantes pour l'objet qui arrivent au même emplacement CloudFront périphérique sont traitées à partir du CloudFront cache.

Déploiement de la solution

Pour déployer cette solution de site web statique sécurisé, vous pouvez choisir l'une des options suivantes :

- Utilisez la CloudFormation console pour déployer la solution avec le contenu par défaut, puis téléchargez le contenu de votre site Web sur Amazon S3.
- Clonez la solution sur votre ordinateur pour ajouter le contenu de votre site web. Puis, déployez la solution avec l’ AWS Command Line Interface (AWS CLI).

> **Note**
>
> Vous devez utiliser la région USA Est (Virginie du Nord) pour déployer le CloudFormation modèle.

Rubriques

- Conditions préalables
- Utiliser la CloudFormation console
- Clonage local de la solution
- Recherche des journaux d'accès

Conditions préalables

Pour utiliser cette solution, les prérequis suivant sont nécessaires :

- Un nom de domaine enregistré, par exemple example.com, pointant vers une zone hébergée Amazon Route 53. La zone hébergée doit se trouver dans le même Compte AWS où vous déployez cette solution. Si vous n'avez pas de nom de domaine enregistré, vous pouvez en

enregistrer un avec Route 53. Si vous possédez un nom de domaine enregistré, mais qu'il ne pointe pas vers une zone hébergée Route 53, configurez Route 53 en tant que votre service DNS.

- Gestion des identités et des accès AWS Autorisations (IAM) pour lancer des CloudFormation modèles qui créent des rôles IAM, et autorisations pour créer toutes les AWS ressources de la solution. Pour plus d'informations, consultez Contrôle de l'accès à l'aide de Gestion des identités et des accès AWS dans le Guide de l'utilisateur AWS CloudFormation .

Vous assumez les coûts encourus pour utiliser cette solution. Pour plus d'informations sur les coûts, consultez les pages de tarification correspondantes Service AWS.

Utiliser la CloudFormation console

Pour déployer à l'aide de la CloudFormation console

1. Lancez cette solution dans la CloudFormation console. Si nécessaire, connectez-vous à votre Compte AWS.
2. L'assistant de création d'une pile s'ouvre dans la CloudFormation console, avec des champs préremplis qui spécifient le CloudFormation modèle de cette solution.

   Au bas de la page, sélectionnez Next.
3. Dans la page Spécifier les détails de la pile, saisissez des valeurs pour les champs suivants :

   - SubDomain— Entrez le sous-domaine à utiliser pour votre site Web. Par exemple, si le sous-domaine est www, votre site Web est disponible à l'adresse *`www.example.com.`* (remplacez exemple.com par votre nom de domaine, comme expliqué dans la bullet suivante.)
   - DomainName— Entrez votre nom de domaine, tel que*`example.com`*. Ce domaine doit pointer vers une zone hébergée Route 53.
   - HostedZoneId— L'ID de zone hébergée Route 53 de votre nom de domaine.
   - CreateApex— (Facultatif) Créez un alias pour le domaine apex (exemple.com) dans votre CloudFront configuration.
4. Lorsque vous avez terminé, choisissez Next (Suivant).
5. (Facultatif) Dans la page Configure stack options (Configurer les options de pile), ajoutez des balises et d'autres options de pile.
6. Lorsque vous avez terminé, choisissez Next (Suivant).

7. Dans la page Vérification, faites défiler jusqu'au bas de la page, puis sélectionnez les deux cases de la section Capacités. Ces fonctionnalités permettent CloudFormation de créer un rôle IAM qui permet d'accéder aux ressources de la pile et de nommer les ressources de manière dynamique.
8. Choisissez Créer une pile.
9. Attendez la fin de la création de la pile. La pile crée des piles imbriquées, ce qui peut prendre plusieurs minutes. Une fois achevée, l'État passe à CREATE_COMPLETE.

   Lorsque le statut est CREATE_COMPLETE, accédez à https ://*www.example.com*pour consulter votre site Web (remplacez www.exemple.com par le sous-domaine et le nom de domaine que vous avez spécifiés à l'étape 3). Vous devriez voir le contenu par défaut du site web :



Pour remplacer le contenu par défaut du site web par le vôtre

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le bucket dont le nom commence par amazon-cloudfront-secure-static-site-s3bucketroot -.

   > **Note**
   >
   > Assurez-vous de choisir le compartiment dont le nom contient s3bucketroot et pas s3bucketlogs. Le compartiment dont le nom inclut s3bucketroot contient le contenu du site web. Celui dont le nom inclut s3bucketlogs ne contient que des fichiers journaux.

3. Supprimez le contenu par défaut du site web, puis chargez le vôtre.

   > **Note**
   >
   > Si vous avez consulté votre site Web avec le contenu par défaut de cette solution, il est probable qu'une partie du contenu par défaut soit mise en cache dans un emplacement CloudFront périphérique. Pour vous assurer que les visiteurs voient le contenu mis à jour de votre site Web, invalidez les fichiers pour supprimer les copies mises en cache

des emplacements CloudFront périphériques. Pour de plus amples informations, veuillez consulter Invalidation de fichiers pour supprimer du contenu.

Clonage local de la solution

Conditions préalables

Pour ajouter votre contenu du site web avant de déployer cette solution, vous devez empaqueter les artefacts de cette dernière localement, ce qui demande Node.js et npm. Pour plus d'informations, consultez https://www.npmjs.com/get-npm.

Pour ajouter votre contenu du site web et déployer la solution

1. Clonez ou téléchargez la solution à partir de https://github.com/aws-samples/amazon-cloudfront-secure-static-site. Après le clonage ou le téléchargement, ouvrez une invite de commande ou un terminal et accédez au dossier `amazon-cloudfront-secure-static-site`.
2. Exécutez la commande suivante pour installer et empaqueter les artefacts de la solution :

```
make package-static
```

3. Copiez votre contenu du site web dans le dossier `www`, en écrasant le contenu par défaut du site web.
4. Exécutez la AWS CLI commande suivante pour créer un compartiment Amazon S3 afin de stocker les artefacts de la solution. *amzn-s3-demo-bucket-for-artifacts*Remplacez-le par votre propre nom de compartiment.

```
aws s3 mb s3://amzn-s3-demo-bucket-for-artifacts --region us-east-1
```

5. Exécutez la AWS CLI commande suivante pour empaqueter les artefacts de la solution sous forme de CloudFormation modèle. *amzn-s3-demo-bucket-for-artifacts*Remplacez-le par le nom du bucket que vous avez créé à l'étape précédente.

```
aws cloudformation package \
    --region us-east-1 \
    --template-file templates/main.yaml \
    --s3-bucket amzn-s3-demo-bucket-for-artifacts \
    --output-template-file packaged.template
```

6. Exécutez la commande suivante pour déployer la solution avec CloudFormation, en remplaçant les valeurs suivantes :

   - *your-CloudFormation-stack-name*— Remplacez par le nom de la CloudFormation pile.
   - *example.com*— Remplacez-le par votre nom de domaine. Ce domaine doit pointer vers une zone hébergée Route 53 dans le même Compte AWS.
   - *www*— Remplacez par le sous-domaine à utiliser pour votre site Web. Par exemple, si le sous-domaine est www, votre site web est disponible à l'adresse www.exemple.com.
   - *hosted-zone-ID*— Remplacez par l'ID de zone hébergée Route 53 de votre nom de domaine.

   ```
   aws cloudformation deploy \
       --region us-east-1 \
       --stack-name your-CloudFormation-stack-name \
       --template-file packaged.template \
       --capabilities CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \
       --parameter-overrides DomainName=example.com SubDomain=www HostedZoneId=hosted-
   zone-ID
   ```

   - (Facultatif) Pour déployer la pile avec un apex de domaine, exécutez plutôt la commande suivante.

     ```
     aws --region us-east-1 cloudformation deploy \
         --stack-name your-CloudFormation-stack-name \
         --template-file packaged.template \
         --capabilities CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \
         --parameter-overrides  DomainName=example.com SubDomain=www
      HostedZoneId=hosted-zone-ID CreateApex=yes
     ```

7. Attendez la fin de la création de la CloudFormation pile. La pile crée des piles imbriquées, ce qui peut prendre plusieurs minutes. Une fois achevée, l'État passe à CREATE_COMPLETE.

   Lorsque le statut passe à CREATE_COMPLETE, accédez https://www.example.com à pour consulter votre site Web (remplacez www.example.com par le sous-domaine et le nom de domaine que vous avez spécifiés à l'étape précédente). Vous devriez voir le contenu de votre site web.

Recherche des journaux d'accès

Cette solution active les journaux d'accès pour la distribution CloudFront. Procédez comme suit pour localiser les journaux d'accès de la distribution.

Pour localiser les journaux d'accès de la distribution

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le bucket dont le nom commence par amazon-cloudfront-secure-static-site-s3bucketlogs -.

   > **Note**
   >
   > Assurez-vous de choisir le compartiment dont le nom contient s3bucketlogs et pas s3bucketroot. Le compartiment dont le nom inclut s3bucketlogs contient des fichiers journaux. Celui dont le nom inclut s3bucketroot contient le contenu du site web.

3. Le dossier nommé cdn contient les journaux CloudFront d'accès.

CloudFront pour les applications de commerce électronique et de place de marché

Une application de commerce électronique ou de place de marché propose trois types de contenu distincts via une seule CloudFront distribution : des actifs statiques (images de produits, CSS JavaScript), des pages dynamiques (listes de produits, résultats de recherche) et des réponses d'API (panier, inventaire, prix). Chaque type de contenu nécessite un comportement de cache, un TTL et une configuration d'origine différents pour trouver un équilibre entre fraîcheur et performances.

Pour les contrôles de sécurité qui s'appliquent aux distributions de sites de vente et de commerce électronique, consultezListe de contrôle de sécurité pour les distributions Marketplace.

Présentation de l’architecture

Une CloudFront distribution Marketplace utilise plusieurs comportements de cache pour acheminer les demandes vers la bonne origine en fonction des modèles de chemin d'URL. Les ressources statiques sont diffusées depuis Amazon Simple Storage Service (Amazon S3), tandis que le contenu dynamique et les demandes d'API sont transférés vers un Elastic Load Balancing (Application Load Balancer) situé devant vos serveurs d'applications. Un cluster ElastiCache (Valkey) fournit un cache au niveau de l'application entre l'ALB et votre base de données pour les données de produit fréquemment consultées.

Composants de l'architecture de distribution

Composant	Contenu diffusé	Objectif
CloudFront distribution	Tout le contenu (domaine unique)	Mise en cache périphérique globale, terminaison TLS, routage des demandes à l'aide de comportements de cache
Origine d'Amazon S3 (actifs statiques)	Images de produits, CSS, JS, polices	Stockage d'objets durable avec contrôle d'accès à l'origine (OAC). Contenu immuable avec de longs TTL.

Composant	Contenu diffusé	Objectif
Origine ALB (contenu dynamique)	Pages de produits, recherche, points de terminaison d'API	Routes vers les serveurs d'applications. TTL courts ou absence de mise en cache pour le contenu personnalisé.
ElastiCache cluster (Valkey)	Catalogue de produits, inventaire, données de session	Application-level cache entre ALB et la base de données. Sub-millisecond lit les données fréquemment consultées.

Comportements du cache pour le commerce électronique

Les comportements du cache déterminent la manière dont CloudFront les requêtes sont traitées en fonction des modèles de chemin d'URL. Pour une place de marché, configurez des comportements distincts pour chaque type de contenu avec des politiques de cache et des TTL appropriés.

Comportements de cache recommandés

Modèle de chemin	Origin	TTL	Politique de cache	Justification
`/static/*`	Amazon S3	365 jours	CachingOptimized	Les noms de fichiers versionnés (par exemple `app.a1b2c3.js`) autorisent un TTL maximal. L'invalidation du cache n'est jamais nécessaire : déployez de nouvelles versions avec de nouveaux noms de fichiers.
`/images/*`	Amazon S3	30 jours	CachingOptimized	Les images des produits changent rarement. Utilisez l'invalidation du cache-tag lorsqu'un vendeur met

Modèle de chemin	Origin	TTL	Politique de cache	Justification
				à jour une image. TTL inférieur à celui des actifs statiques car les URL des images peuvent être réutilisées.
`/api/products/*`	ALB	60 secondes	Personnalisé (inclure les chaînes de requête)	Les API de liste de produits et de recherche changent fréquemment mais tolèrent une brève obsolescence. Incluez les paramètres de chaîne de requête dans la clé de cache pour la pagination et les filtres.
`/api/cart/*`	ALB	0 (pas de cache)	CachingDisabled	Les opérations du panier sont spécifiques à l'utilisateur et doivent toujours atteindre l'origine. Désactivez complètement la mise en cache.
`/api/inventory/*`	ALB	5 secondes	Personnalisé (inclure les chaînes de requête)	Les inventaires changent rapidement pendant les événements de vente. Le TTL très court empêche les surventes tout en réduisant la charge d'origine.

Modèle de chemin	Origin	TTL	Politique de cache	Justification
`Default (*)`	ALB	0 (pas de cache)	CachingDisabled	Le comportement par défaut transmet les requêtes non mises en cache à l'application pour un rendu côté serveur. Les pages qui incluent du contenu personnalisé (recommandations, nom d'utilisateur) ne doivent pas être mises en cache en périphérie.

> **Note**
>
> Organisez les comportements du cache du plus spécifique au moins spécifique. CloudFront évalue les modèles de trajectoire dans l'ordre indiqué et utilise la première correspondance. Placez `/api/cart/*` avant `/api/*` pour vous assurer que les demandes de panier contournent la mise en cache.

Pour plus d'informations sur les comportements de cache, consultez the section called “Paramètres de comportement du cache”.

Stratégie TTL pour le contenu du marché

La configuration TTL détermine la durée pendant laquelle le contenu mis en cache CloudFront est conservé avant de vérifier l'origine des mises à jour. E-commerce les applications nécessitent différentes stratégies TTL en fonction de l'impact de la fraîcheur du contenu sur l'expérience client.

Ressources immuables (CSS, JS, polices)

Définissez le TTL maximum (365 jours). Utilisez des noms de fichiers dont le contenu est haché afin que chaque déploiement crée de nouvelles URL. N'invalidez jamais : les anciennes versions

expirent naturellement lorsque les utilisateurs chargent les nouveaux noms de fichiers. Fixé `Cache-Control: public, max-age=31536000, immutable` à l'origine.

Images du produit

Définissez le TTL sur 30 jours avec invalidation de la balise de cache lors de la mise à jour. Lorsqu'un vendeur télécharge une nouvelle image, invalidez-la par la balise cache du produit plutôt que par le chemin. Cela cible uniquement les objets concernés sans invalidation générale des caractères génériques. Fixé `Cache-Control: public, max-age=2592000` à l'origine.

API du catalogue de produits

Réglez TTL sur 60 secondes. Les listes de produits, les descriptions et les prix tolèrent une brève obsolescence. Cela réduit la charge d'origine lors des pics de trafic (ventes flash, lancements de produits) tout en maintenant les données raisonnablement à jour. `Cache-Control: public, max-age=60, stale-while-revalidate=30`Paramétré pour diffuser du contenu obsolète tout en CloudFront récupérant une nouvelle réponse en arrière-plan.

API d'inventaire et de tarification

Réglez TTL sur 5 secondes. Ces valeurs changent fréquemment et influent sur les décisions d'achat. Une mise en cache très courte réduit toujours la charge d'origine de plusieurs ordres de grandeur lors des pics de trafic : des milliers d'utilisateurs simultanés voient la même réponse en cache de 5 secondes au lieu que chacun d'entre eux atteigne l'origine.

User-specific contenu (panier, recommandations)

Désactivez la mise en cache (TTL = 0). Le contenu qui varie d'un utilisateur à l'autre doit toujours atteindre son origine. Si vous mettez en cache par erreur du contenu spécifique à un utilisateur, CloudFront il est possible que les données d'un utilisateur soient transmises à un autre utilisateur. Utilisez la politique `CachingDisabled` gérée pour ces comportements.

Configuration d'origine

Amazon S3 Origin pour les actifs statiques

Utilisez un compartiment Amazon S3 comme source pour les images de produits et les ressources statiques. Configurez le contrôle d'accès à l'origine (OAC) pour restreindre l'accès direct au compartiment : toutes les demandes doivent y être CloudFront acheminées.

Paramètres d'origine d'Amazon S3

Paramètre	Value	Justification
Domaine de l’origine	`marketplace-assets.s3.amazonaws.com`	Utilisez le point de terminaison de l'API REST Amazon S3 (et non le point de terminaison du site Web) pour prendre en charge l'OAC.
Accès à l’origine	Contrôle d'accès à l'origine (OAC)	Limite l'accès au bucket CloudFront uniquement à. Empêche l'accès direct à vos ressources par URL S3.
Bouclier d'origine	Activé (région la plus proche du compartiment)	Ajoute une couche de mise en cache centralisée entre les emplacements périphériques et l'origine. Réduit les coûts des requêtes S3 et améliore le taux d'accès au cache pour les images.
Connection attempts (Tentatives de connexion)	3	Par défaut. Réessaie en cas d'erreurs S3 transitoires.

Origine ALB pour le contenu dynamique

Utilisez un équilibreur de charge d'application comme source pour les pages de produits dynamiques, les recherches et les points de terminaison d'API. L'ALB est acheminé vers vos serveurs d'applications (instances Amazon EC2, tâches Amazon ECS ou fonctions Lambda à l'aide de groupes cibles).

Paramètres d'origine ALB

Paramètre	Value	Justification
Domaine de l’origine	Nom DNS ALB	Utilisez directement le nom DNS ALB. N'utilisez pas d'adresse IP : les adresses IP ALB changent.

Paramètre	Value	Justification
Protocole	HTTPS Only	Chiffre le trafic entre CloudFron t et l'origine. Nécessaire pour les données sensibles (sessions utilisate ur, informations de paiement).
En-tête personnalisé Origin	`X-Origin-Verify: <secret-value>`	Limite l'accès à ALB aux demandes provenant de. CloudFront L'ALB vérifie cet en-tête et rejette les tentatives d'accès direct.
Délai de connexion	10 secondes	Plus court que la valeur par défaut (30s). Échouez rapidement en cas de problèmes d'origine au lieu de faire attendre les connexions Edge.
Délai de réponse	30 secondes	Permet de consacrer du temps aux requêtes de recherche complexes et aux opérations de catalogue . Augmentez cette valeur si les opérations de votre API sont prolongées.
Keep-alive délai d'attente	5 secondes	Réutilise les connexions à l'ALB. Réduit les frais d'établissement de contacts TLS pour les demandes suivantes.

Application-level mise en cache avec ElastiCache (Valkey)

CloudFront met en cache le contenu à la périphérie, mais les données fréquemment consultées qui nécessitent des requêtes de base de données bénéficient d'un cache supplémentaire au niveau de l'application. Un ElastiCache cluster exécutant Valkey se trouve entre vos serveurs d'applications et la base de données, fournissant des lectures inférieures à la milliseconde des données du catalogue de produits, des inventaires et de l'état des sessions.

Two-tier stratégie de mise en cache

Couche	Ce qu'il met en cache	TTL	Comportement des erreurs de cache
CloudFront bord	Réponses HTTP complètes (API JSON, pages HTML, images)	5s — 365d (par comportement)	Transfère la demande à l'origine ALB
ElastiCache (Vallée)	Objets de données d'application (fiches produits, inventaire, sessions)	30 s à 5 min (par type de données)	L'application interroge la base de données et écrit le résultat dans le cache

Sur une demande de page produit :

1. CloudFront vérifie son cache périphérique. En cas d'activation, renvoie immédiatement la réponse mise en cache.
2. En cas d'échec, CloudFront il passe à l'ALB.
3. L'application vérifie ElastiCache les données du produit. En cas d'accès, génère la réponse à partir des données mises en cache (en dessous de la milliseconde).
4. En cas d' ElastiCache échec, interroge la base de données ElastiCache, écrit dans et renvoie la réponse.
5. CloudFront met en cache la réponse à la périphérie en fonction du paramètre TTL du comportement.

Lorsqu'un vendeur met à jour un produit :

1. L'application invalide la clé de produit dans. ElastiCache
2. L'application envoie un cache-tag d'invalidation à CloudFront pour le tag du produit.
3. La requête suivante déclenche une nouvelle réponse via les deux couches de cache.

Questions fréquentes (FAQ)

Les sections suivantes répondent aux questions courantes concernant les stratégies de mise en cache pour les charges de travail du commerce électronique et des places de marché.

Comment gérer le contenu personnalisé grâce à la mise en cache ?

Séparez les éléments personnalisés du contenu pouvant être mis en cache. Diffusez l'enveloppe de la page (détails du produit, images, descriptions) depuis le CloudFront cache et chargez des éléments personnalisés (recommandations, nombre de paniers, nom d'utilisateur) en utilisant des appels d'API côté client qui contournent la mise en cache. Avec cette approche, vous pouvez mettre en cache le rendu de page coûteux et maintenir la personnalisation à jour.

Comment choisir entre l'invalidation et les TTL courts ?

Utilisez des TTL courts (5 à 60 secondes) pour le contenu qui change fréquemment et de manière prévisible (inventaire, prix). Utilisez l'invalidation pour le contenu qui change rarement mais qui doit être mis à jour immédiatement lorsqu'il le fait (images de produits après modification par un vendeur, descriptions de produits après examen de conformité). L'invalidation a un coût par demande et une limite de simultanéité. Ne l'utilisez pas comme substitut aux TTL appropriés.

Comment me préparer aux ventes flash et aux pics de trafic ?

CloudFront évolue automatiquement pour gérer les pics de trafic. Pour optimiser le taux d'accès au cache pendant une vente : préchauffez les pages des produits en les demandant avant le début de l'événement, augmentez temporairement le TTL des API (par exemple, augmentez le TTL de l'inventaire de 5 à 15 s) pour absorber plus de trafic en périphérie, et assurez-vous que votre ElastiCache cluster dispose d'une marge de mémoire suffisante pour augmenter les écritures dans le cache. Surveillez la métrique du taux d'accès du CloudFront cache pendant l'événement.

Dois-je utiliser Origin Shield pour mon site de vente ?

Oui. Origin Shield ajoute une couche de cache centralisée entre les caches périphériques régionaux et votre origine. Pour les charges de travail du commerce électronique, elle réduit les demandes d'origine pour les produits les plus populaires (car un accès au cache d'Origin Shield dessert tous les emplacements périphériques), réduit les coûts S3 GET pour les images et atténue les pics de trafic vers l'ALB. Activez-le dans la région la plus proche de votre lieu d'origine. Pour plus d'informations, consultez the section called “Utilisation d’Origin Shield”.

Liste de contrôle de sécurité pour les distributions Marketplace

E-commerce et les applications de la place de marché gèrent des données sensibles : sessions clients, flux de paiement et contenu premium. Cette liste de contrôle couvre les contrôles de sécurité spécifiques à une CloudFront distribution dotée d'une couche de mise en cache ElastiCache (Valkey). Appliquez ces contrôles en plus des bonnes pratiques générales CloudFront de sécurité décrites dansConfiguration d'un accès sécurisé et restriction de l'accès au contenu.

Cette liste de contrôle complète les instructions de configuration contenues dansCloudFront pour les applications de commerce électronique et de place de marché.

URL signées et cookies pour le contenu premium

Utilisez des URL signées ou des cookies signés pour restreindre l'accès au contenu nécessitant une autorisation : aperçus de produits premium, produits numériques achetés, contenu promotionnel limité dans le temps ou ressources spécifiques au vendeur.

Comparaison des URL signées et des cookies signés

Méthode	À utiliser lorsque	E-commerce exemple
URL signée	Restreindre l'accès à des fichiers individuels. Partage de liens de téléchargement. Les clients qui n'acceptent pas les cookies.	One-time lien de téléchargement pour un produit numérique acheté. Time-limitedaccès à une image de produit en haute résolution pour un vendeur vérifié.
Cookie signé	Fournir un accès à plusieurs fichiers (par exemple, tous les actifs d'un niveau premium). Éviter les modifications d'URL pour le contenu existant.	Accès à un catalogue complet de contenus numériques en tant que membre Premium. Subscriber-only des aperçus de produits sur plusieurs pages.

Exigences de configuration :

- Créez un groupe de clés avec une clé publique RSA (2048 bits minimum). Stockez la clé privée AWS Secrets Manager pour que votre application génère des signatures.
- Définissez le comportement du cache sur Oui pour Restreindre l'accès des spectateurs et associez le groupe de clés.
- Définissez un délai d'expiration adapté au type de contenu : minutes pour les liens de téléchargement, heures pour les sessions de navigation, jours pour l'accès à l'abonnement.
- Utilisez une politique personnalisée (et non une politique prédéfinie) lorsque vous devez restreindre par plage d'adresses IP ou autoriser des chemins d'accès par caractères génériques.

Pour plus d'informations sur l'implémentation, consultez the section called “Restriction de contenu avec des URL et des cookies signés”.

Contrôle d'accès à l'origine (OAC) pour Amazon S3

Le contrôle d'accès Origin empêche les utilisateurs CloudFront d'accéder directement à votre compartiment Amazon S3. Sans OAC, toute personne qui découvre l'URL de votre bucket peut accéder aux actifs sans passer par votre URL/cookie application signée, les règles WAF ou les restrictions géographiques. Pour connaître les étapes de configuration complètes, consultezthe section called “Restreindre l'accès à un AWS origine”.

Activez l'OAC pour toutes les origines Amazon S3

Créez un OAC et associez-le à chaque origine Amazon S3 de votre distribution. Mettez à jour la politique de compartiment pour autoriser uniquement le principal de CloudFront service (`cloudfront.amazonaws.com`) dont la condition correspond à votre ARN de distribution.

Supprimer l'accès public

Dans la console Amazon Simple Storage Service, activez Amazon S3 Block Public Access sur le bucket. Il s'agit d'un paramètre Amazon S3, pas d'un CloudFront paramètre. La politique du compartiment n'autorise l'accès qu'à CloudFront : aucune ACL ou politique publique n'est nécessaire. Pour plus d'informations, consultez la section Bloquer l'accès public à votre stockage Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Utiliser le point de terminaison de l'API REST Amazon S3

Configurez l'origine à l'aide du point de terminaison de l'API REST du bucket (`bucket-name.s3.amazonaws.com`), et non du point de terminaison du site Web Amazon S3. L'OAC fonctionne uniquement avec le point de terminaison de l'API REST.

Chiffrement en transit

Chiffrez toutes les connexions dans le chemin de la demande : le visualiseur vers CloudFront, CloudFront vers l'origine et l'application vers ElastiCache le cache.

Configuration du chiffrement en transit

Connexion	Paramètre	Configuration
Afficheur → CloudFront	Politique relative au protocole de visualisation : HTTPS uniquement	Définissez la politique du protocole de visualisation `https-only` sur `redirect-to-https` ou sur tous les comportements du cache. Utilisez une politique de sécurité minimale TLS 1.2 (`TLSv1.2_2021`).
CloudFront → Origine S3	Protocole d'origine : HTTPS	Les points de terminaison de l'API REST S3 prennent en charge le protocole HTTPS par défaut. CloudFront utilise HTTPS lorsque vous configurez l'origine avec le point de terminaison de l'API REST et l'OAC.
CloudFront → Origine ALB	Protocole d'origine : HTTPS uniquement	Définissez la politique du protocole d'origine sur`https-only` . Installez un certificat TLS valide sur l'ALB (utilisez AWS Certificate Manager). CloudFront valide le certificat lors de la connexion.
Candidature → ElastiCache	In-transit chiffrement : Activé	Dans la ElastiCache console, activez l'option `TransitEncryptionE nabled` sur le groupe de réplicati on. Il s'agit d'un ElastiCache réglage. Utilisez les connexions TLS à partir du code de votre application. Valkey et Redis OSS 6.0 et versions

Connexion	Paramètre	Configuration
		ultérieures prennent en charge le chiffrement en transit de manière native.

Groupes de sécurité VPC pour le cluster de cache

Le ElastiCache cluster s'exécute dans un VPC et ne doit accepter que les connexions provenant de vos serveurs d'applications. Utilisez le chaînage des groupes de sécurité pour restreindre l'accès.

Configuration du groupe de sécurité pour ElastiCache

Groupe de sécurité	Règle entrante	Justification
Cluster de cache SG	TCP 6379 à partir de l'application SG uniquement	Seuls les serveurs d'applications peuvent accéder au cache. Pas d'accès à Internet, pas d'accès à d'autres services. Utilisez le port 6379 (Valkey/Redis port par défaut) ou le port que vous avez configuré.
Application SG	TCP 443 depuis ALB SG uniquement	Les serveurs d'applications n'acceptent que le trafic provenant de l'ALB. Combiné au cluster de cache SG, cela crée une chaîne : CloudFront → ALB → App → Cache.

Durcissement supplémentaire en PVC :

- Déployez le ElastiCache cluster dans des sous-réseaux privés sans route de passerelle Internet.
- Utilisez un groupe de sous-réseaux qui couvre au moins deux zones de disponibilité pour une haute disponibilité.
- Activez ElastiCache le jeton d'authentification (mot de passe) pour une couche d'authentification supplémentaire au-delà des groupes de sécurité.
- Désactivez l'accès public au ElastiCache cluster (par défaut, mais vérifiez).

Contrôles de sécurité supplémentaires

Restreindre l'accès à CloudFront ALB uniquement

Ajoutez un en-tête d'origine personnalisé (`X-Origin-Verify`) qui est CloudFront envoyé avec chaque demande. Configurez l'ALB ou l'application pour rejeter les demandes qui n'incluent pas cet en-tête. Stockez la valeur de l'en-tête AWS Secrets Manager et faites-la pivoter périodiquement. Vous pouvez également utiliser la liste de préfixes CloudFront gérés pour limiter les règles entrantes des groupes de sécurité ALB aux CloudFront plages d'adresses IP.

Activer AWS WAF sur la distribution

Associez une ACL AWS WAF Web à des règles de limitation de débit pour vous protéger contre les abus de panier, le remplissage d'informations d'identification sur les API de connexion et le grattage de l'inventaire. Utilisez des groupes de règles gérés pour les menaces courantes (injection SQL, XSS) et des règles personnalisées pour les modèles spécifiques aux applications.

Geo-restrictions à des fins de conformité

Si votre site de vente est présent dans certains pays, activez la géo-restriction pour bloquer les demandes provenant de régions où vous n'êtes pas légalement autorisé à vendre ou à expédier. Postulez au niveau de la distribution. Pour la restriction géographique par chemin, utilisez des conditions de AWS WAF géo-correspondance dans une règle ACL Web avec une condition de chemin d'URL.

Journalisation des accès

Activez la journalisation CloudFront standard ou la journalisation en temps réel pour détecter les modèles d'accès anormaux : pics soudains d'utilisation des liens de téléchargement, accès depuis des régions inattendues ou tentatives d'authentification échouées répétées aux points de terminaison de l'API.

CloudFront plans tarifaires forfaitaires

CloudFront les plans tarifaires forfaitaires combinent le réseau CloudFront mondial de diffusion de contenu (CDN) d'Amazon avec de multiples fonctionnalités Services AWS et dans un prix mensuel sans frais d'excédent, indépendamment des pics de trafic ou des attaques.

Flat-rate les plans tarifaires incluent les fonctionnalités suivantes pour un tarif mensuel simple :

- CloudFront CDN
- AWS WAF et protection contre les attaques DDoS
- Gestion et analyse des bots
- DNS Amazon Route 53
- Ingestion d'Amazon CloudWatch Logs
- Certificat TLS
- Calcul de périphérie sans serveur
- Crédits de stockage Amazon S3 par mois

Les plans sont disponibles dans les niveaux Free, Pro, Business et Premium pour répondre aux besoins de votre application. Les forfaits ne nécessitent pas d'engagement annuel pour obtenir les meilleurs tarifs disponibles. Commencez par le plan gratuit et passez à la version supérieure pour accéder à davantage de fonctionnalités et à des limites d'utilisation plus importantes.

Rubriques

- Avantages des plans tarifaires CloudFront forfaitaires
- Fonctionnalités par niveau de plan tarifaire
- Allocations d'utilisation mensuelles
- Coûts couverts par votre plan
- Réduire globalement AWS coûts liés aux plans tarifaires
- Gérez vos plans tarifaires forfaitaires
- Permissions
- Flat-rate quotas de plans tarifaires
- Fonctions non prises en charge

Avantages des plans tarifaires CloudFront forfaitaires

Le plan CloudFront tarifaire offre plusieurs avantages clés :

- Services et prix consolidés

  Combinez plusieurs Services AWS fonctionnalités en un seul plan pour un tarif forfaitaire. Conçu pour éliminer les achats de services séparés et les calculs de prix initiaux.
- Pas de dépassement

  Il n'y a pas de frais d'utilisation excédentaire, qu'il s'agisse de pics de trafic ou d'attaques.
- Autorisations d'utilisation claires

  Chaque plan comprend des allocations d'utilisation publiées conçues pour des performances optimales à ce niveau. Surveillez votre utilisation, recevez des notifications proactives et effectuez la mise à niveau en fonction des besoins de votre application, sans engagement à long terme.
- Protégez-vous contre les attaques DDoS

  CloudFront et AWS WAF absorbez et bloquez les attaques avant qu'elles n'atteignent votre infrastructure. Réserve l'utilisation de votre calcul, de votre base de données et de votre infrastructure uniquement pour le trafic légitime. Les attaques DDoS bloquées et les demandes bloquées par AWS WAF ne sont jamais prises en compte dans votre allocation d'utilisation.
- Réduisez vos AWS coûts globaux

  Le transfert de données depuis AWS des applications exécutées sur des services tels qu'Amazon S3, AWS Application Load Balancer (ALB) ou Amazon API Gateway est CloudFront toujours gratuit. Lorsque vous diffusez vos AWS applications via Internet CloudFront plutôt que directement, votre forfait couvre les coûts de transfert de données entre vos applications et vos spectateurs pour un simple prix mensuel, sans vous soucier des dépassements. La diminution du nombre de demandes qui parviennent à votre point d'origine réduit également vos coûts sur les services facturés en fonction de l'utilisation.

Fonctionnalités par niveau de plan tarifaire

Chaque plan tarifaire couvre une CloudFront distribution avec jusqu'à un domaine apex (racine) qui combine des fonctionnalités et des services essentiels en un seul prix mensuel. Chaque plan inclut également des crédits de stockage S3 supplémentaires.

Les plans des niveaux supérieurs incluent toutes les fonctionnalités des plans de niveau inférieur ainsi que des fonctionnalités supplémentaires.

- Gratuit — Pour les amateurs, les apprenants et les développeurs débutants.
- Pro — Lancez et développez de petits sites Web, des blogs et des applications.
- Business : protégez et accélérez les applications métier.
- Premium : adaptez et protégez les applications professionnelles et stratégiques.

Sélectionnez un niveau de plan qui inclut les fonctionnalités et les configurations dont vous avez besoin pour vos applications. Consultez les fonctionnalités suivantes par plan tarifaire.

Caractéristiques du plan tarifaire

Le tableau suivant présente les CloudFront fonctionnalités AWS WAF et les fonctionnalités DDoS d'Amazon Route 53 CloudWatch, Amazon et Amazon S3 incluses dans chaque niveau de plan tarifaire.

Performances et livraison	Free	Pro	Entreprise	Prime
CDN mondial	Oui	Oui	Oui	Oui
Utilisez CloudFront plus de 750 sites périphériques mondiaux comme point d'entrée massif, distribué et unique pour votre application Web. Accélérez les applications statiques, dynamiques et	✓	✓	✓	✓

Performances et livraison	Free	Pro	Entreprise	Prime
ne pouvant pas être mises en cache.				

Performances et livraison	Free	Pro	Entreprise	Prime
Mise en cache du contenu Stockez des copies de votre contenu dans plus de CloudFront 750 sites périphériques du monde entier, en les diffusant aux utilisateurs depuis l'emplacement le plus proche. Réduit les temps de chargement, protège votre application contre les pics de trafic et réduit les coûts en traitant les demandes répétées localement plutôt que depuis vos serveurs d'applications.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Invalidations rapides du cache Supprimez ou mettez à jour le contenu mis en cache dans tous les emplacements périphériques en quelques secondes.	Oui 	Oui 	Oui 	Oui 
Invalidations par balise de cache Attribuez des balises personnalisées à votre contenu et supprimez tout le contenu mis en cache partagean t une étiquette spécifique, sans suivre les chemins de fichiers individue ls.		Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Routage intelligent Achemine intelligemment les utilisateurs vers l'emplacement périphérique optimal à l'aide de données réseau en temps réel, et se connecte à votre AWS point d'origine via le réseau AWS privé pour de meilleures performances.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Mise en cache hiérarchisée [Les caches périphériques régionaux sont] placés entre les emplacements périphériques et votre application afin de stocker le contenu plus longtemps, de réduire la charge de votre application et de garantir une diffusion rapide.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Règles de mise en cache par défaut	Oui 	Oui 	Oui 	Oui 
Prend des décisions efficaces en matière de mise en cache pour mettre en cache la plupart des applications Web sans configuration personnalisée.				

Performances et livraison	Free	Pro	Entreprise	Prime
Règles de mise en cache personnalisées Contrôlez la manière dont le contenu est mis en CloudFront cache en spécifiant les valeurs de requête à utiliser, en optimisant les performances, la personnalisation et les besoins de mise à jour de votre application à l'aide de politiques de cache.			Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
High-speed routage d'origine Avec Origin Shield, les demandes dynamiques sont acheminées depuis des emplacements périphériques vers votre point d'origine via CloudFront un réseau privé pour un chemin performant vers votre origine.				Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Réduction de la charge d'origine Ajoute une couche de mise en cache supplémentaire à proximité de votre application Web à l'aide d'Origin Shield. Origin Shield consolide les demandes provenant de tous les emplacements périphériques, réduisant ainsi la charge de votre application, en particulier pendant les pics de trafic.				Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Basculement automatique de l'origine Achemine automatiquement le trafic vers une origine de sauvegarde en cas de défaillance de votre origine principale, afin de maintenir une haute disponibilité sans perturber les utilisateurs.				Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Règles de demande d'origine par défaut Contrôlez quelles informations provenant des requêtes des spectateurs sont automatiquement incluses dans les demandes adressées à votre origine, à l'aide de politiques de demande d'origine AWS gérées optimisées pour les scénarios courants.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Règles d'en-tête de réponse par défaut	Oui 	Oui 	Oui 	Oui 
Utilisez des politiques d'en-tête de réponse AWS gérées pour ajouter ou supprimer des en-têtes HTTP dans les réponses aux utilisateurs, préconfigurées pour les en-têtes de sécurité courants, les paramètres CORS et d'autres cas d'utilisation standard.				

Performances et livraison	Free	Pro	Entreprise	Prime
Règles de demande d'origine personnalisées			Oui	Oui
Créez vos propres politiques de demande d'origine pour spécifier exactement quelles chaînes de requête URL, quels en-têtes et quels cookies sont transférés vers votre origine, afin de permettre des analyses et une gestion des demandes personnalisées.			✓	✓

Performances et livraison	Free	Pro	Entreprise	Prime
Règles d'en-tête de réponse personnalisées Créez vos propres politiques d'en-tête de réponse pour contrôler exactement quels en-têtes HTTP sont ajoutés ou CloudFront supprimés dans les réponses aux utilisateurs, tels que les en-têtes de sécurité, la politique de sécurité du contenu (CSP), les paramètres CORS et les en-têtes d'application personnalisés.			Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Nombre de comportements de cache	5	10	50	100
Configurez les comportements du cache pour contrôler la façon dont CloudFront les demandes relatives à des modèles d'URL spécifiques sont gérées, notamment l'origine du contenu, la manière dont le contenu est mis en cache et si des URL HTTPS ou signées sont requises.				
Sécurité et protection				

Performances et livraison	Free	Pro	Entreprise	Prime
Always-on Protection contre les attaques DDoS Protégez-vous contre les attaques DDoS qui ciblent vos sites Web ou vos applications.	Oui ✓	Oui ✓	Oui ✓	Oui ✓
Protection DDoS avancée Identifiez et bloquez les attaques DDoS en quelques secondes grâce à l'AntiDDoS AMR. AWS apprend les modèles uniques de vos applications pour faire la distinction entre les attaques et les poussées naturelles provenant d'utilisateurs légitimes.			Oui ✓	Oui ✓

Performances et livraison	Free	Pro	Entreprise	Prime
Pare-feu d'application Web (WAF) Protégez-vous contre les vulnérabilités courantes des applications et les menaces potentielles grâce aux renseignements internes sur les menaces d'Amazon. Les requêtes sont bloquées avant d'atteindre vos serveurs.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Nombre de règles WAF	5	25	50	75
Nombre total de règles de sécurité que vous pouvez créer et activer dans votre configuration WAF, y compris les règles personnalisées et les règles AWS gérées.				

Performances et livraison	Free	Pro	Entreprise	Prime
Protections pour WordPress les bases de données PHP et SQL		Oui 	Oui 	Oui 
Use-case règles de sécurité basées sur des règles de sécurité pour protéger les applications et les systèmes d'exploitation courants tels que PHP WordPress , les bases de données SQL, Linux et Windows.				

Performances et livraison	Free	Pro	Entreprise	Prime
Analyse du trafic par IA Surveillez les modèles d'accès, les volumes de demandes et les chemins populaires des robots IA qui interagissent avec votre contenu. Les robots IA sont classés en fonction de leur intention de détecter des activités telles que le scraping potentiellement non autorisé utilisé à des fins d'entraînement.		Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
IP-based limitation de débit Bloquez automatiquement les adresses IP qui dépassent un nombre configurable de requêtes sur une période de 5 minutes, afin de vous protéger contre les attaques par inondation HTTP et les tentatives de déni de service (DoS).	Oui 	Oui 	Oui 	Oui 
Blocage du trafic géographique Bloquez les demandes provenant de pays ou de régions sélectionnés.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Défi CAPTCHA		Oui	Oui	Oui
Exiger des requêtes répondant à des règles de sécurité spécifiques pour résoudre un puzzle CAPTCHA afin de prouver qu'un être humain envoie la demande.		✓	✓	✓
Header-based filtrage des menaces		Oui	Oui	Oui
Créez des règles de sécurité WAF qui filtrent les menaces en fonction des en-têtes de requêtes HTTP.		✓	✓	✓

Performances et livraison	Free	Pro	Entreprise	Prime
Regex-based filtrage des menaces			Oui	Oui
Créez des règles de sécurité WAF à l'aide d'expressions régulières pour faire correspondre les chemins URI et les attributs des requêtes HTTP.			✓	✓
JavaScript défi			Oui	Oui
Bloquez les menaces automatisées en demandant aux navigateurs de relever des JavaScript défis qui vérifient la légitimité des utilisateurs.			✓	✓

Performances et livraison	Free	Pro	Entreprise	Prime
Gestion et analyse des bots (+robots IA)			Oui	Oui
Détectez et analysez le trafic des robots avec AWS WAF Bot Control pour les robots courants. Fournit des contrôles pour bloquer, contester ou autoriser les robots non vérifiés tout en identifiant et en distingua nt les robots vérifiés tels que les moteurs de recherche . Surveillez les robots dotés d'IA et prenez des mesures en fonction de leur intention.			✓	✓

Performances et livraison	Free	Pro	Entreprise	Prime
Réponse WAF personnalisée Définissez un code d'état HTTP spécifique et, en option, une réponse HTML personnalisée, texte brut ou JSON lorsque les requêtes sont bloquées par une règle.		Oui 	Oui 	Oui 
Insertion d'en-tête Ajoutez des en-têtes HTTP personnalisés aux requêtes qui réussissent l'inspection WAF, afin de permettre aux applications en aval de traiter les demandes différemment ou de les signaler pour analyse.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Demander une inspection corporelle	16 Ko	16 Ko	64 Ko	64 Ko
Taille maximale du contenu du corps de requête HTTP qui peut être inspecté AWS WAF pour détecter les menaces et les modèles malveillants.				
Origines privées au sein de VPC			Oui	Oui
Renforcez la sécurité en conservant votre application dans un sous-réseau privé VPC, accessible uniquement via vos CloudFront distributions et masqué de l'Internet public, à l'aide des origines du VPC.			✓	✓

Performances et livraison	Free	Pro	Entreprise	Prime
TLS mutuel (origine) Limitez l'accès non autorisé à votre application (origine) à l'aide de certificats TLS-based clients, en vous assurant que seules vos CloudFront distributions autorisées peuvent établir des connexions avec votre application.			Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Contrôle d'accès à l'origine (OAC) Conservez un compartiment S3 privé et n'autorisez l'accès que via la CloudFront distribution que vous avez désignée, en vous assurant que votre contenu est protégé par vos règles WAF, vos limites de débit et les autres contrôles de sécurité configurés dans votre CloudFront distribution.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Certificat TLS gratuit Certificat TLS gratuit pour votre domaine avec renouvellement automatique via AWS Certificate Manager.	Oui 	Oui 	Oui 	Oui 
URL signées Créez des URL sécurisées qui fournissent un accès temporaire au contenu privé pour des utilisateurs spécifiques. Généralement utilisé pour partager des documents privés avec des utilisateurs autorisés ou accorder un accès sécurisé à du contenu protégé après vérification du paiement.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
TLS mutuel (mTLS) Restreignez l'accès à votre application à l'aide de l'authentification mTLS, en vous assurant que seuls les clients de confiance dotés de certificats valides peuvent se connecter.				Oui 
Edge Compute				

Performances et livraison	Free	Pro	Entreprise	Prime
Calcul de périphérie sans serveur Exécutez Lightweight JavaScript at the Edge pour modifier les URL, les en-têtes HTTP et les request/response éléments en quelques millisecondes à l'aide de Functions. CloudFront Lambda @Edge peut également être utilisé avec tous les niveaux de forfait, mais contrairement à CloudFron t Functions , les appels Lambda @Edge sont facturés sur la base du paiement à l'utilisation.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Magasin de valeurs clés Edge		Oui	Oui	Oui
Stockez les données à la périphérie KeyValueStore pour une personnalisation rapide et dynamique du contenu grâce à CloudFront Functions.		✓	✓	✓
Support réseau et protocole				

Performances et livraison	Free	Pro	Entreprise	Prime
IPv6 Diffusez du contenu via des connexions IPv6 modernes et IPv4 traditionnelles, CloudFront à destination des spectateurs et des sites d'origine. Permet une prise en charge IPv6 de bout en bout pour vos applications.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
HTTP/2 Accélérez le chargement des pages grâce à des fonctionnalités de protocole modernes telles que le multiplexage, la compression d'en-tête et la hiérarchisation des flux. Utilisé automatiquement lorsqu'il est pris en charge par les navigateurs et les clients.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
HTTP/3 Diffusez du contenu à l'aide de QUIC aux navigateurs et aux clients qui le prennent en charge, afin d'accélérer les connexions et d'améliorer les performances. Cela profite particulièrement aux utilisateurs mobiles et permet de maintenir les connexions lorsque les conditions du réseau changent.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
TLS 1.3 Fournissez des connexions HTTPS plus rapides grâce à un processus d'établissement de contacts qui nécessite un aller-retour, contre deux dans TLS 1.2. Réduit la latence du premier octet jusqu'à 33 % par rapport aux versions TLS précédentes. Activé de bout en bout pour vos applications.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
WebSockets Activez une communication bidirectionnelle permanente et en temps réel entre les navigateurs et les serveurs. Idéal pour les applications de chat IA, les jeux multijoueurs, les espaces de travail collaboratifs et les flux de données en temps réel tels que les plateformes de trading financier.	Oui 	Oui 	Oui 	Oui 
Consignation et surveillance				

Performances et livraison	Free	Pro	Entreprise	Prime
Journaux d'accès Accédez à des journaux de CloudFront demandes détaillés pour comprendre les modèles de trafic de sécurité et de livraison. L'ingestion d'Amazon CloudWatch Logs est incluse sans frais supplémentaires.		Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Journaux des requêtes WAF Accédez à des journaux de AWS WAF demandes détaillés pour comprendre les modèles de trafic de sécurité et de livraison . L'ingestion d'Amazon CloudWatch Logs est incluse sans frais supplémentaires.		Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
Tableau de bord de sécurité Surveillez les événements de sécurité, étudiez les menaces et prenez des mesures de blocage immédiates à l'aide de l'analyse visuelle sans écrire de règles de sécurité. Les versions Pro et ultérieures incluent un analyseur visuel des journaux pour comprendre rapidement les modèles de trafic sans interroger les journaux.	Oui 	Oui 	Oui 	Oui 
DNS				

Performances et livraison	Free	Pro	Entreprise	Prime
DNS Amazon Route 53 Service DNS d'autorité publique rapide et fiable utilisant Route 53.	Oui 	Oui 	Oui 	Oui 
Enregistrements par zone hébergée Le nombre maximum d'enregistrements DNS autorisés dans la zone hébergée.	50	100	1 000	5000

Performances et livraison	Free	Pro	Entreprise	Prime
DNSSEC Protégez votre domaine contre l'usurpation du DNS et les attaques de type « man-in-the-middle », dans le cadre desquelles les attaquants interceptent les requêtes DNS et redirigent les visiteurs vers de faux sites Web. Sécurise le trafic DNS en signant de manière cryptographique vos enregistrements DNS.	Oui	Oui	Oui	Oui
Stockage				

Performances et livraison	Free	Pro	Entreprise	Prime
Stockage Amazon S3	5 Go	50 Go	1 To	5 To
Des crédits de stockage Amazon S3 qui compensent tous les coûts de stockage S3 Standard dans votre Compte AWS. Non limité au CloudFront contenu et soumis aux limites d'utilisation du plan.				
Support et fiabilité				

Performances et livraison	Free	Pro	Entreprise	Prime
Assistance en matière de compte et de facturation 24 h/24 et 7 j/7	Oui	Oui	Oui	Oui
One-on-one réponses aux questions relatives au compte et à la facturation.				
Si vous avez un plan d'assistance payant, vous pouvez bénéficier d'une assistance sur tous les plans forfaitaires.				

Performances et livraison	Free	Pro	Entreprise	Prime
Documentation et AWS Support forums Accédez à la documentation des produits, à des documents techniques, à des guides de bonnes pratiques, à des forums AWS re:Post communautaires et à des informations sur l'état des services pour vous aider à planifier et à résoudre les problèmes.	Oui 	Oui 	Oui 	Oui 

Performances et livraison	Free	Pro	Entreprise	Prime
SLA de disponibilité Les contrats de niveau de service (SLA) pour Amazon CloudFront AWS WAF, Amazon Route 53 et Amazon CloudWatch prévoient des engagements en matière de disponibilité des services. Si l'engagement du SLA associé AWS n'est pas respecté, vous aurez droit à un crédit de service.			Oui ✓	Oui ✓

Allocations d'utilisation mensuelles

Chaque plan forfaitaire comprend une allocation d'utilisation mensuelle conçue pour des performances optimales à ce niveau. Les allocations d'utilisation ne sont pas des limites strictes : elles représentent l'utilisation de base que votre plan est conçu pour prendre en charge. Vous pouvez suivre votre consommation dans la CloudFront console à tout moment et vous recevrez des notifications automatiques par e-mail lorsque vous atteindrez 50 %, 80 % et 100 % de votre allocation.

Allocations d'utilisation mensuelles par niveau de forfait

	Free	Pro	Entreprise	Prime
Requêtes	1 M	10 M	125 M	500 M (configurable jusqu'à 6 B pour un nouveau prix forfaitaire)
Transfert de données	100 Go	50 TO	50 TO	50 To (configurable jusqu'à 600 To pour un nouveau prix forfaitaire)

Qu'est-ce qui compte pour votre allocation d'utilisation

Les attaques DDoS bloquées et les demandes bloquées par AWS WAF ne sont jamais prises en compte dans votre allocation d'utilisation. Seul le trafic qui dépasse vos règles AWS WAF de sécurité est pris en compte pour votre allocation. Cela signifie que les attaques et le trafic indésirable ne seront pas pris en compte contre vous, et vous conservez la possibilité de définir exactement le trafic que votre application bloque ou autorise.

Que se passe-t-il lorsque l'utilisation dépasse l'allocation

Les plans sont conçus pour être flexibles et s'adapter aux modèles de trafic réels tels que la variabilité du trafic, la croissance organique et les événements viraux. Plus important encore : vous n'aurez pas à payer de frais d'excédent, quel que soit le montant que vous dépassez votre allocation. Si votre utilisation dépasse votre allocation en raison d'une croissance soutenue sur plusieurs mois ou d'une utilisation anormalement élevée en un mois, la distribution de votre trafic peut être ajustée. La plupart des clients ne constatent jamais d'ajustements de performance.

Voici comment cela fonctionne :

- Votre premier pic de trafic, jusqu'à 3 fois votre allocation mensuelle, n'affectera pas votre service ce mois-là. Cet hébergement ponctuel gère les événements inattendus tels que le contenu viral ou les lancements de produits réussis sans pénaliser votre succès.

- Une utilisation prolongée supérieure à votre allocation est évaluée sur une période de 2 à 3 mois ou plus, et non pas immédiatement. Des fluctuations mineures et une croissance modérée sont attendues et prises en compte. Seule une utilisation excessive importante et durable indique que votre application a dépassé votre niveau.
- Vous recevrez des notifications chaque mois lorsque vous vous approchez de votre allocation et que vous la dépasserez. Si votre consommation dépasse régulièrement et de manière significative votre forfait, nous vous recommandons de passer à un niveau qui correspond à votre croissance et garantit des performances optimales au fur et à mesure de votre évolution. Vous contrôlez vos performances en effectuant des mises à niveau lorsque vos habitudes d'utilisation de base changent.
- Si vous continuez à dépasser largement l'allocation d'utilisation de votre forfait sans effectuer de mise à niveau, la distribution de votre trafic peut être ajustée. Par exemple, votre trafic peut être desservi depuis des sites périphériques moins nombreux ou plus éloignés, ou les performances peuvent être ajustées. Le degré d'ajustement est proportionnel : un léger excédent de consommation entraîne des changements minimes, un excédent plus important et soutenu entraîne des changements plus visibles. La mise à niveau permet de rétablir toutes les performances.

La plupart des clients ne constatent jamais d'ajustements de performance. Les plans sont conçus pour s'adapter aux modèles de croissance normaux.

Allocations d'utilisation configurables sur le plan Premium

Le plan Premium propose des allocations d'utilisation mensuelles configurables par distribution. Lorsque vous souscrivez ou gérez un forfait Premium, vous pouvez sélectionner une allocation d'utilisation mensuelle plus élevée parmi les niveaux suivants :

Niveaux d'utilisation premium

Niveau d'utilisation Premium	Transfert de données mensuel	Demandes mensuelles	Flat-rate prix par mois
Premium (par défaut)	50 TO	500 MÈTRES	1 000$
Prime	75 T	750 MÈTRES	1 450$
Prime	125 TONNES	1,25 G	2 250$

Niveau d'utilisation Premium	Transfert de données mensuel	Demandes mensuelles	Flat-rate prix par mois
Prime	200 TONNES	2 B	3 500$
Prime	350 TONNES	3,5 GO	6 000$
Prime	600 TONNES	6 B	10 000$

Lorsque vous sélectionnez un niveau d'utilisation plus élevé, votre prix mensuel augmente et votre allocation d'utilisation mensuelle augmente en conséquence. Les fonctionnalités et services inclus dans le plan Premium restent les mêmes à tous les niveaux d'utilisation. Vous modifiez uniquement votre allocation d'utilisation et votre prix forfaitaire. Les mêmes politiques d'allocation d'utilisation s'appliquent à tous les niveaux d'utilisation. Pour plus de détails, consultez Que se passe-t-il lorsque l'utilisation dépasse l'allocation.

Vous pouvez modifier votre niveau d'utilisation à tout moment dans la CloudFront console. Lorsque vous augmentez votre niveau d'utilisation, les modifications prennent effet immédiatement. Votre prix et votre allocation d'utilisation sont calculés au prorata. Lorsque vous diminuez votre niveau d'utilisation, la modification prend effet au début du cycle de facturation suivant.

Si l'utilisation de base de votre application dépasse 6 milliards de demandes ou 600 To par mois, contactez-nous pour obtenir une tarification personnalisée.

> **Note**
>
> Les allocations d'utilisation configurables ne sont disponibles que sur le plan Premium. Les limites d'utilisation des forfaits Free, Pro et Business ne sont pas configurables.

Éligibilité basée sur l'utilisation historique

Votre historique CloudFront d'utilisation peut affecter votre éligibilité à souscrire à des niveaux de plan spécifiques ou à passer à des niveaux de forfait spécifiques. Si votre utilisation récente dépasse les limites d'utilisation d'un niveau de forfait, vous devrez peut-être sélectionner un niveau supérieur mieux adapté à votre charge de travail.

Coûts couverts par votre plan

Votre plan couvre les coûts suivants :

- Votre CloudFront distribution
- L'ACL AWS WAF Web, les règles personnalisées, les règles AWS gérées et les frais de demande pour l'ACL Web associée à votre distribution
- CloudWatch Ingestion des journaux pour les journaux d' CloudFront accès de votre distribution et les journaux WAF associés
- La zone hébergée Route 53, les enregistrements DNS et les requêtes DNS lorsqu'ils sont associés au plan de distribution

Vous recevrez également des crédits S3 pour compenser l'utilisation du stockage S3 Standard sur votre compte payeur, qu'un compartiment S3 soit utilisé ou non comme origine de votre CloudFront distribution.

La gestion du DNS Route 53 et votre plan

Si vous utilisez Route 53 pour le DNS et que vous associez la zone à votre forfait, votre forfait peut inclure les coûts de votre zone hébergée Route 53. Vous pouvez associer la zone à votre plan dans la section Gérer le plan de votre CloudFront distribution. Lorsque votre zone est associée au plan, celui-ci couvre les coûts standard de votre zone hébergée, y compris les frais mensuels de zone hébergée, les enregistrements DNS et les frais de requête DNS, sous réserve des allocations respectives par niveau, indiquées ci-dessous. La zone hébergée doit répondre aux exigences suivantes :

- Exister dans le même AWS compte que votre CloudFront distribution
- Conservez le nombre d'enregistrements autorisés par zone hébergée pour le niveau de votre plan
- Couvrez le domaine utilisé par votre CloudFront distribution

Si votre zone hébergée n'est pas associée à votre forfait, elle restera facturée à l'utilisation, selon laquelle vous serez responsable de tous les coûts standard de la Route 53.

Comprendre les allocations mensuelles de requêtes DNS

Lorsque votre zone hébergée est associée à votre forfait, vous bénéficiez de :

1. Requêtes DNS vers des enregistrements ALIAS pointant vers votre CloudFront distribution et d'autres enregistrements pris en charge Services AWS
2. Une allocation mensuelle supplémentaire pour les autres types d'enregistrements DNS

	Free	Pro	Entreprise	Prime
Requêtes DNS vers les enregistrements ALIAS (CloudFront et autres enregistrements pris en charge Services AWS) par mois	Aucune limite	Aucune limite	Aucune limite	Aucune limite
Allocation de requêtes DNS supplémentaire par mois	1 M	5 M	20 M	100 M

> **Note**
>
> Pour optimiser les avantages de votre plan, utilisez les enregistrements ALIAS pour indiquer votre CloudFront distribution. Les enregistrements ALIAS pointant vers CloudFront et autres enregistrements pris en charge Services AWS ne sont pas pris en compte dans votre allocation mensuelle de requêtes DNS. Toutes les autres requêtes DNS, y compris les enregistrements CNAME vers CloudFront, sont prises en compte dans votre allocation de requêtes DNS.

Dépassement des autorisations de requêtes DNS

Si l'utilisation de vos requêtes DNS dépasse l'allocation mensuelle de votre forfait, vous AWS pourriez vous en informer. À ce stade, vous pouvez détacher votre zone hébergée du plan dans la

section Gérer le plan de votre CloudFront distribution pour rétablir la tarification de la zone hébergée à l'utilisation. Si vous ne détachez pas votre zone hébergée après avoir reçu cette notification, AWS il est possible que la zone hébergée passe automatiquement à une tarification à l'utilisation. Lorsqu'une zone hébergée passe à la tarification à l'utilisation, vous êtes responsable de tous les coûts standard de la Route 53. Votre CloudFront distribution et tous les autres avantages du plan restent inchangés.

Réduire globalement AWS coûts liés aux plans tarifaires

CloudFront les plans tarifaires forfaitaires peuvent réduire vos AWS coûts globaux de trois manières :

Tout d'abord, les coûts de transfert de données entre CloudFront et vos AWS applications exécutées sur des services tels qu'Amazon S3, AWS Application Load Balancer (ALB) ou Amazon API Gateway sont automatiquement annulés. Lorsque vous diffusez vos AWS applications via Internet CloudFront plutôt que directement, votre forfait couvre les coûts de transfert de données entre vos applications et vos spectateurs pour un simple prix mensuel, sans vous soucier des dépassements.

Deuxièmement, CloudFront réduisez vos coûts de calcul et de base de données en protégeant l'infrastructure de vos applications et en réduisant le nombre de requêtes atteignant votre origine. Il diffuse du contenu mis en cache à partir d'emplacements périphériques ou de caches périphériques régionaux, réduit les demandes dupliquées et bloque le trafic malveillant et indésirable avant qu'il n'atteigne vos services principaux. Cela signifie qu'il y a moins de requêtes sur vos serveurs d'applications, bases de données et autres Services AWS qui sont facturées en fonction de l'utilisation, ce qui réduit vos coûts.

Enfin, chaque plan inclut des crédits de stockage Amazon S3 Standard pour compenser l'utilisation de votre espace de stockage Compte AWS.

Pour optimiser ces économies, configurez vos AWS origines de manière à n'accepter que le trafic en provenance deCloudFront. Pour S3, utilisez Origin Access Control OAC avec des compartiments privés pour accorder l'accès à la distribution que vous avez désignée CloudFront. Pour les instances Application Load Balancer, Network Load Balancer et Amazon EC2 dans des sous-réseaux privés, limitez l'accès à la CloudFront distribution que vous avez désignée à l'aide de VPC Origins.

Gérez vos plans tarifaires forfaitaires

Vous pouvez gérer vos plans tarifaires CloudFront forfaitaires à l'aide de la CloudFront console ou de manière programmatique à l'aide du AWS Command Line Interface (AWS CLI) ou de l'API.

PricingPlanManager Cette section explique comment souscrire des distributions à des plans tarifaires, modifier les niveaux des plans et annuler des abonnements à l'aide de la CloudFront console.

Pour plus d'informations sur la gestion des plans tarifaires par programmation, consultez la section Premiers pas avec l' PricingPlanManager API.

Souscrire une nouvelle distribution à un plan tarifaire

Lorsque vous créez une nouvelle distribution, vous pouvez souscrire à un plan tarifaire.

Pour souscrire une nouvelle distribution à un plan tarifaire

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Distributions, puis suivez les étapes pour créer une distribution.
3. Choisissez le plan tarifaire de votre distribution. Notez que certaines fonctionnalités ne sont pas disponibles par niveau de plan tarifaire. Passez en revue les fonctionnalités de chaque plan et choisissez le plan tarifaire dont vous avez besoin pour votre application.
4. Suivez les étapes pour créer votre distribution.

Souscrire une distribution existante à un plan tarifaire

Lorsque vous mettez à jour une distribution, vous pouvez souscrire à un plan tarifaire. Avant de choisir un plan tarifaire, assurez-vous que votre configuration de distribution est compatible avec le plan que vous souhaitez.

> **Tip**
>
> Si votre distribution actuelle utilise des fonctionnalités non prises en charge, vous devez désactiver ces fonctionnalités avant de pouvoir souscrire au plan tarifaire. Cela inclut la désactivation de fonctionnalités telles que les journaux d'accès en temps réel.

Une fois que votre configuration de distribution est compatible, vous pouvez choisir le plan tarifaire souhaité tout en mettant à jour une distribution.

Pour souscrire une distribution existante à un plan tarifaire

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Distributions, puis suivez les étapes pour mettre à jour une distribution existante.
3. Choisissez le plan tarifaire de votre distribution. Notez que certaines fonctionnalités ne sont pas disponibles par niveau de plan tarifaire. Passez en revue les fonctionnalités de chaque plan et choisissez le plan tarifaire dont vous avez besoin pour votre application.
4. Suivez les étapes pour mettre à jour votre distribution.

Mettre à niveau un plan tarifaire

Nous vous recommandons de passer à un forfait si vous approchez ou avez dépassé votre limite d'utilisation mensuelle, ou si vous souhaitez activer une fonctionnalité disponible au niveau suivant.

Lorsque vous passez à un niveau de plan supérieur, les modifications prennent effet immédiatement. Votre prix et votre allocation d'utilisation sont calculés au prorata. Votre distribution et les ressources associées auront accès aux fonctionnalités disponibles et à l'allocation d'utilisation plus élevée de votre nouveau forfait.

Pour mettre à niveau un plan tarifaire

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez votre distribution qui est souscrite à un plan tarifaire existant.
4. Suivez les instructions pour mettre à niveau le plan tarifaire de votre distribution.
5. Suivez les étapes pour mettre à jour une distribution existante.

Modifier le niveau d'utilisation de votre forfait Premium

Si vous êtes abonné au forfait Premium, vous pouvez modifier votre niveau d'utilisation pour augmenter ou diminuer votre allocation d'utilisation.

Lorsque vous augmentez votre niveau d'utilisation, la modification prend effet immédiatement et votre prix est calculé au prorata. Lorsque vous diminuez votre niveau d'utilisation, la modification prend effet au début du cycle de facturation suivant.

Pour modifier le niveau d'utilisation de votre forfait Premium

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez votre distribution qui est souscrite à un plan tarifaire Premium.
4. Cliquez sur le bouton Gérer le plan.
5. Dans la section Gérer le plan, choisissez Modifier le plan.
6. Suivez les instructions pour modifier votre niveau d'utilisation pour le plan tarifaire Premium. La console affiche les niveaux d'utilisation disponibles et les prix mensuels correspondants.

Rétrograder un plan tarifaire

Nous vous recommandons de passer à un niveau de forfait inférieur si vous n'avez pas besoin des fonctionnalités supplémentaires de votre niveau existant. Par exemple, vous pouvez passer à une version antérieure si vous pensez que le trafic de votre application diminuera.

Si vous passez à un niveau inférieur, vos modifications de facturation prendront effet au début du prochain cycle de facturation.

Si votre distribution dépasse actuellement l'allocation d'utilisation d'un forfait, vous pouvez passer à une version inférieure une fois que votre utilisation se situe dans les limites de l'allocation d'utilisation du niveau souhaité. Pour éviter d'être facturé pour le niveau de votre forfait actuel lors du prochain cycle de facturation, passez à un forfait inférieur avant la fin du mois.

Pour rétrograder un plan tarifaire

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez votre distribution qui est souscrite à un plan tarifaire existant.

4. Suivez les instructions pour rétrograder le plan tarifaire de votre distribution. Si vous disposez de fonctionnalités non prises en charge, vous devez supprimer la fonctionnalité ou la ressource de la distribution.
5. Suivez les étapes pour mettre à jour une distribution existante.

Annuler un plan tarifaire

Lorsque vous annulez un plan tarifaire payant, vous conservez votre prix forfaitaire jusqu'à la fin de votre cycle de facturation en cours. Votre distribution et toutes les ressources associées à votre forfait passeront ensuite à la tarification à l'utilisation au début du prochain cycle de facturation. Les forfaits gratuits sont annulés immédiatement.

Pour annuler un plan tarifaire

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez votre distribution qui est souscrite à un plan tarifaire existant.
4. Suivez les instructions pour annuler le plan tarifaire de votre distribution.
5. Suivez les étapes pour mettre à jour une distribution existante.

Annuler un changement de plan en cours

Si vous avez rétrogradé ou annulé votre plan tarifaire forfaitaire, vous devez attendre la fin du cycle de facturation en cours pour que vos modifications prennent effet. Pour conserver votre plan tarifaire forfaitaire existant, le surclasser ou le rétrograder à nouveau, vous devez d'abord annuler le changement de forfait en cours.

Pour annuler un changement de plan tarifaire en cours

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez votre distribution qui est souscrite à un plan tarifaire existant.
4. Suivez les instructions pour annuler le changement de plan en attente de votre distribution.

5. Choisissez le plan tarifaire que vous souhaitez pour votre distribution.
6. Suivez les étapes pour mettre à jour une distribution existante.

Supprimer une distribution avec un plan tarifaire

Vous ne pouvez pas supprimer une distribution qui est souscrite à un plan tarifaire. Vous devez d'abord annuler le plan tarifaire. Les annulations des plans tarifaires payants prennent effet après le cycle de facturation en cours. Les forfaits gratuits sont annulés immédiatement. Une fois le plan annulé, vous pouvez supprimer la distribution.

Pour supprimer une distribution associée à un plan tarifaire

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Suivez les étapes précédentes pour annuler le plan tarifaire de la distribution.
4. Suivez les étapes pour supprimer la distribution.

> **Note**
>
> Vous pouvez désactiver une distribution qui est souscrite à un plan tarifaire, mais ce plan vous facturera tout de même des frais. Pour ne plus encourir de frais pour votre plan, vous devez d'abord l'annuler.

Permissions

Pour consulter ou gérer les abonnements aux plans tarifaires de vos CloudFront distributions, vous devez disposer des autorisations requises. Pour plus d'informations, consultez AWS politique gérée : CloudFrontFullAccess et AWS politique gérée : CloudFrontReadOnlyAccess.

Flat-rate quotas de plans tarifaires

Le tableau suivant indique les quotas et les restrictions applicables aux plans tarifaires CloudFront forfaitaires.

> **Note**
>
> Ces quotas ne peuvent pas être augmentés pour vous Compte AWS.

Account-level quotas	Quotas
Plans tarifaires par Compte AWS	100
Plans gratuits par Compte AWS	3
Apex-level domaines par plan	1

Fonctions non prises en charge

Avant de pouvoir associer une distribution à un plan tarifaire, vous devez vous assurer que certaines fonctionnalités sont désactivées et que les associations sont supprimées.

> **Remarques**
>
> - Si votre distribution ou votre compte comporte l'une de ces restrictions, vous devez les résoudre avant de pouvoir utiliser des plans tarifaires. Après avoir apporté des modifications à votre distribution, attendez que les modifications se propagent à tous les emplacements périphériques.
> - Une ACL AWS WAF Web doit être associée à votre distribution si vous utilisez un plan tarifaire. Cette ressource ne peut pas être supprimée ou dissociée de votre distribution à moins que vous ne passiez à une tarification à l'utilisation pour cette distribution.

Fonctions non prises en charge

Vous ne pouvez pas souscrire des distributions à un plan tarifaire si leur configuration contient les fonctionnalités non prises en charge suivantes. Vous pouvez désactiver la fonctionnalité non prise en charge et utiliser une autre option, ou conserver le paiement à l'utilisation pour votre distribution.

Fonctions non prises en charge	Options alternatives	Service AWS
Multi-tenantdistributions	Utilisez une distribution standard ou une tarification à l'utilisation	CloudFront
Déploiement continu et distributions intermédiaires	Utilisez la tarification à l'utilisation	CloudFront
Configuration de la liste IP Anycast	Utilisez la tarification à l'utilisation	CloudFront
Real-time journaux d'accès	Utilisez des journaux d'accès standard ou une tarification à l'utilisation	CloudFront
Bots ciblés	Utilisez des robots courants ou une tarification à l'utilisation	AWS WAF
Règles gérées par les partenaires	Utilisez la tarification à l'utilisation	AWS WAF
Création de compte et prévention des fraudes	Utilisez la tarification à l'utilisation	AWS WAF
Protection contre le piratage de compte	Utilisez la tarification à l'utilisation	AWS WAF
Groupes de règles	Créez des règles individuelles (les groupes de règles sont des AWS WAF règles partagées qui peuvent être appliquées à une ACL Web,	AWS WAF

Fonctions non prises en charge	Options alternatives	Service AWS
	de la même manière que les politiques surCloudFront)	
Fonctionnalités héritées		
Configuration de l'Forwarded Values	Utiliser les politiques relatives aux requêtes Origin	CloudFront
Dédié IP/SSL	Utilisez la tarification à l'utilisation	CloudFront
Chiffrement au niveau du champ	Utilisez la tarification à l'utilisation	CloudFront
Certificats de serveur de Gestion des identités et des accès AWS (IAM)	Certificats d'utilisation AWS Certificate Manager (ACM)	CloudFront
Identité d'accès à l'origine (OAI)	Utiliser le contrôle d'accès Origin (OAC)	CloudFront
Paramètres de cache hérités	Utilisez les politiques de cache et les politiques de demande d'origine.	CloudFront

Associations non soutenues

Vous ne pouvez pas souscrire une distribution à un plan tarifaire si la distribution est déjà associée à l'une des ressources suivantes qui sont déjà associées à d'autres distributions. Les ressources associées à une distribution souscrite à un plan tarifaire ne peuvent être utilisées que pour cette distribution. Par exemple, si une CloudFront fonction utilise un magasin de valeurs clés, ni la fonction

ni le magasin de valeurs clés ne peuvent être partagés pour une distribution soumise à un plan tarifaire.

- CloudFront Fonctions
- CloudFront Fonctions associées à un magasin de valeurs clés
- AWS WAF ACL Web

Pour souscrire une distribution à un plan tarifaire, supprimez la ressource associée ou remplacez-la par une autre.

Account-level contraintes

Comptes AWS ne sont pas éligibles aux plans tarifaires s'ils répondent à l'une des conditions suivantes :

- Vous avez atteint le nombre maximum d'abonnements autorisés. Consultez Flat-rate quotas de plans tarifaires.
- Votre compte utilise Niveau gratuit d'AWS.

Resource-level contraintes

Les distributions ne sont pas éligibles aux plans tarifaires si elles répondent à l'une des conditions suivantes :

- Votre distribution a été activée AWS Shield Advanced
- Votre distribution a activé le service Firewall Manager pour votre ACL Web. Firewall Manager ne gérera pas la WebACL de votre CloudFront distribution dans le cadre d'un plan tarifaire.

Fonctionnalités supplémentaires susceptibles d'affecter votre plan tarifaire

Flat-rate les plans tarifaires vous permettent de payer un tarif forfaitaire pour votre CloudFront distribution et les fonctionnalités répertoriées ci-dessus qui sont à la fois incluses dans votre plan et associées à votre CloudFront distribution. Toutes les autres fonctionnalités peuvent entraîner des frais supplémentaires, y compris, mais sans s'y limiter, les suivantes :

CloudFront

- Invocations de la fonction Lambda @Edge

AWS WAF

- Les puzzles CAPTCHA créés à l'aide de l'JavaScript API sont facturés selon une tarification à l'utilisation. Les réponses CAPTCHA configurées dans vos AWS WAF règles (le cas d'utilisation le plus courant) sont incluses dans votre forfait sans frais supplémentaires.

Route 53

- La Route 53 (DNSSEC) a un coût AWS KMS
- Blocs IP (CIDR) de la Route 53 (les 1 000 premiers sont gratuits pour chaque Compte AWS bloc)
- Bilans de santé de la Route 53 (les 50 premiers sont gratuits par personne Compte AWS)

Fonctionnalités de journalisation

- Journaux de requêtes DNS Route 53, journaux de CloudFront fonctions et journaux de fonctions de CloudFront connexion
- AWS WAF envoi de journaux à Amazon S3
- CloudFront ou envoi de AWS WAF journaux à Amazon Data Firehose
- CloudWatch Indicateurs supplémentaires pour CloudFront
- CloudFront journaux d'accès au format Parquet

> **Note**
>
> Votre plan inclut l'ingestion d'Amazon CloudWatch Logs pour les journaux CloudFront standard (journaux d'accès) et les journaux WAF sans frais supplémentaires. Tous les autres CloudWatch coûts tels que le stockage et les requêtes ne sont pas couverts par votre forfait. Tous les autres journaux sont également facturés séparément.

> **Note**
>
> Votre plan inclut le DNS public faisant autorité depuis la Route 53. Lorsque votre zone hébergée Route 53 est associée à votre plan tarifaire, celui-ci couvre les coûts standard de votre zone hébergée, y compris les frais mensuels de zone hébergée, les enregistrements DNS et les frais de requêtes DNS, sous réserve des allocations respectives par niveau. Tous les autres coûts liés à l'utilisation de la Route 53 et aux fonctionnalités non répertoriées ci-dessus et inclus dans votre forfait ne sont pas couverts par votre forfait.

Plans tarifaires par rapport à la tarification à l'utilisation

Flat-rate les forfaits et la tarification à l'utilisation offrent différents avantages en fonction de vos besoins. Avec les forfaits, vous payez un prix unique qui inclut l'ingestion de plusieurs fichiers Services AWS tels CloudFront que Route 53 et CloudWatch Logs, et vous n'avez jamais à payer de frais d'excédent, même en cas de pic de trafic ou d'attaque. AWS WAF

Avec la tarification à l'utilisation, vous êtes facturé séparément pour chaque service et chaque fonctionnalité en fonction de votre utilisation réelle. Bien que cela offre une flexibilité totale dans la sélection et la configuration des services, vos coûts peuvent varier d'un mois à l'autre en fonction des tendances du trafic, et vous devrez surveiller l'utilisation de plusieurs services pour gérer les coûts.

Flat-rate les forfaits sont idéaux si vous souhaitez une facturation mensuelle combinée, une configuration de service simplifiée et des fonctionnalités de sécurité intégrées sans vous soucier des frais d'excédent. Pay-as-you-go la tarification est un meilleur choix si vous avez besoin d'un contrôle total sur les fonctionnalités individuelles des services, des configurations personnalisées, l'accès à des fonctionnalités non disponibles dans les forfaits, ou si vous prévoyez de gérer des pics de trafic importants et prévisibles. Les plans tarifaires CloudFront forfaitaires Amazon ne peuvent être combinés à aucune autre offre, promotion ou remise.

Configuration des distributions

Vous créez une CloudFront distribution Amazon pour indiquer CloudFront d'où vous souhaitez que le contenu soit diffusé, ainsi que les informations relatives au suivi et à la gestion de la diffusion du contenu.

Lorsque vous créez votre CloudFront distribution, configure CloudFront automatiquement la plupart des paramètres de distribution pour vous, en fonction du type d'origine de votre contenu. Pour en savoir plus sur les paramètres précédents, consultez Référence des paramètres de distribution préconfigurés. Vous pouvez, si vous le souhaitez, modifier manuellement les paramètres de votre distribution. Pour plus d'informations, consultez Référence de tous les paramètres de distribution.

Les paramètres suivants peuvent être configurés :

- L'origine de votre contenu : le compartiment, le AWS Elemental MediaPackage canal, le AWS Elemental MediaStore conteneur, l'équilibreur de charge Elastic Load Balancing ou le serveur HTTP Amazon S3 à partir CloudFront duquel les fichiers doivent être distribués. Vous pouvez spécifier n'importe quelle combinaison pouvant aller jusqu'à 25 origines pour une distribution unique.
- Accès : si vous voulez que l'accès aux fichiers soit possible pour tout le monde ou si vous souhaitez le restreindre à certains utilisateurs.
- Sécurité : si vous souhaitez activer la protection AWS WAF et exiger des utilisateurs qu'ils emploient le protocole HTTPS pour accéder à votre contenu. Pour les distributions multi-locataires, seules les listes de contrôle d'accès Web (ACL) AWS WAF V2 sont prises en charge.
- Clé de cache : valeurs, le cas échéant, que vous souhaitez inclure dans la clé de cache. La clé de cache identifie de manière unique chaque fichier du cache pour une distribution donnée.
- Paramètres de la demande d'origine : si vous CloudFront souhaitez inclure des en-têtes HTTP, des cookies ou des chaînes de requête dans les demandes envoyées à votre origine.
- Restrictions géographiques : si vous CloudFront souhaitez empêcher les utilisateurs de certains pays d'accéder à votre contenu.
- Journaux : que vous souhaitiez CloudFront créer des journaux standard ou des journaux d'accès en temps réel qui indiquent l'activité des spectateurs.

Pour plus d'informations, consultez Référence de tous les paramètres de distribution.

Pour connaître le nombre maximal actuel de distributions que vous pouvez créer pour chacune d'elles Compte AWS, consultezQuotas généraux sur les distributions. Il n'y a pas de nombre maximum de fichiers que vous pouvez servir par distribution.

Vous pouvez utiliser des distributions pour diffuser le contenu suivant via HTTP ou HTTPS :

- Contenu de téléchargement statique et dynamique, tel que des fichiers HTML JavaScript, CSS et images, via HTTP ou HTTPS.
- La vidéo à la demande dans différents formats, notamment Apple HTTP Live Streaming (HLS) et Microsoft Smooth Streaming. (Smooth Streaming n'est pas pris en charge pour les distributions multi-locataires.) Pour plus d'informations, consultez Diffusez des vidéos à la demande avec CloudFront.
- Un événement en direct, tel qu'une réunion, une conférence ou un concert en temps réel. Pour le streaming en direct, vous pouvez créer la distribution automatiquement à l'aide d'une CloudFormation pile. Pour plus d'informations, consultez Diffusez des vidéos en streaming avec CloudFront et AWS Services multimédias.

Les rubriques suivantes fournissent plus de détails sur les CloudFront distributions et sur la manière de les configurer pour répondre aux besoins de votre entreprise. Pour plus d'informations sur la création d'une distribution, reportez-vous à Créer une distribution.

Rubriques

- Compréhension du fonctionnement des distributions multi-locataires
- Créer une distribution
- Référence des paramètres de distribution préconfigurés
- Référence de tous les paramètres de distribution
- Test d'une distribution
- Mettre à jour une distribution
- Marquer une CloudFront ressource
- Supprimer une distribution
- Utilisez différentes origines avec les CloudFront distributions
- Activer IPv6 pour les CloudFront distributions
- Utilisez le déploiement CloudFront continu pour tester en toute sécurité les modifications de configuration du CDN

- Utilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME)
- Utilisation WebSockets avec les CloudFront distributions
- Demande d'adresses IP statiques en unidiffusion à utiliser pour la liste d'autorisation
- Utilisation de gRPC avec des distributions CloudFront

Compréhension du fonctionnement des distributions multi-locataires

Vous pouvez créer des distributions CloudFront multi-locataires avec des paramètres qui peuvent être réutilisés entre plusieurs locataires de distribution. Dans le cas d'une distribution mutualisée, vous pouvez CloudFront configurer vos paramètres de distribution pour vous, en fonction du type d'origine de votre contenu. Pour en savoir plus sur les paramètres précédents, consultez Référence des paramètres de distribution préconfigurés.

Pour déplacer une distribution standard existante vers une distribution multi-locataires, voirMigration vers une distribution multi-locataires.

L'utilisation d'une distribution multi-locataires plutôt qu'une distribution standard présente les avantages suivants :

- Réduction de la charge opérationnelle.
- Configurations réutilisables permettant aux administrateurs Web et aux fournisseurs de logiciels de gérer CloudFront la distribution de plusieurs applications Web fournissant du contenu aux utilisateurs finaux.
- Intégrations améliorées avec d'autres solutions Services AWS pour fournir une gestion automatisée des certificats, des contrôles de sécurité unifiés et un contrôle de configuration à grande échelle sans tracas.
- Maintien de modèles de ressources cohérents dans l'ensemble de vos implémentations. Définissez les paramètres qui doivent être partagés, puis indiquez les personnalisations à appliquer à ceux qui doivent être remplacés.
- Paramètres d'origine et de sécurité personnalisables pour répondre à des besoins spécifiques au niveau du locataire de distribution.
- Organisez vos locataires de distribution en différents niveaux. Par exemple, si certains locataires de distribution ont besoin d'Origin Shield et d'autres non, vous pouvez regrouper les locataires de distribution dans différentes distributions multi-locataires.

- Partage d’une configuration DNS commune sur plusieurs domaines.

Contrairement à une distribution standard, une distribution multi-locataires n'est pas directement accessible car elle ne possède pas de point de terminaison CloudFront de routage. Elle doit donc être utilisée conjointement avec un groupe de connexion et un ou plusieurs locataires de distribution. Bien que les distributions standard aient leur propre CloudFront point de terminaison et soient directement accessibles aux utilisateurs finaux, elles ne peuvent pas être utilisées comme modèle pour d'autres distributions.

Pour plus d’informations sur les quotas de distribution multi-locataires, consultez Quotas sur les distributions multi-locataires.

Rubriques

- Comment ça marche
- Termes
- Fonctions non prises en charge
- Personnalisations du locataire de distribution
- Demandez des certificats pour votre locataire CloudFront de distribution
- Création d’un groupe de connexions personnalisé (facultatif)
- Migration vers une distribution multi-locataires

Comment ça marche

Une distribution standard regroupe tous les paramètres que vous souhaitez activer pour votre site web ou votre application, notamment les configurations d’origine, les comportements du cache et les paramètres de sécurité. Si vous souhaitez créer un site web différent tout en conservant de nombreux paramètres identiques, vous devez créer une nouvelle distribution à chaque fois.

CloudFront Les distributions multi-locataires sont différentes dans la mesure où vous pouvez créer une distribution multi-locataires initiale. Pour chaque nouveau site web, vous créez un locataire de distribution qui hérite automatiquement des valeurs définies dans sa distribution source. Vous personnalisez ensuite des paramètres spécifiques pour votre locataire de distribution.

Vue d’ensemble

1. Pour commencer, vous devez d'abord créer une distribution multi-locataires. CloudFront configure vos paramètres de distribution pour vous, en fonction du type d'origine de votre contenu. Vous

pouvez personnaliser les paramètres pour toutes les origines, à l'exception des origines VPC. Les paramètres des origines VPC sont personnalisés directement sur la ressource d'origine VPC elle-même. Pour plus d'informations sur les paramètres de distribution multi-locataires que vous pouvez personnaliser, consultez Référence des paramètres de distribution préconfigurés.

- Le certificat TLS que vous utilisez pour la distribution multi-locataires peut être hérité par vos locataires de distribution. La distribution multi-locataires elle-même n'est pas routable ; aucun nom de domaine ne peut donc lui être associé.

2. Par défaut, CloudFront crée un groupe de connexion pour vous. Le groupe de connexion contrôle la manière dont les demandes de contenu des utilisateurs se connectent CloudFront. Vous pouvez personnaliser certains paramètres de routage dans le groupe de connexions.

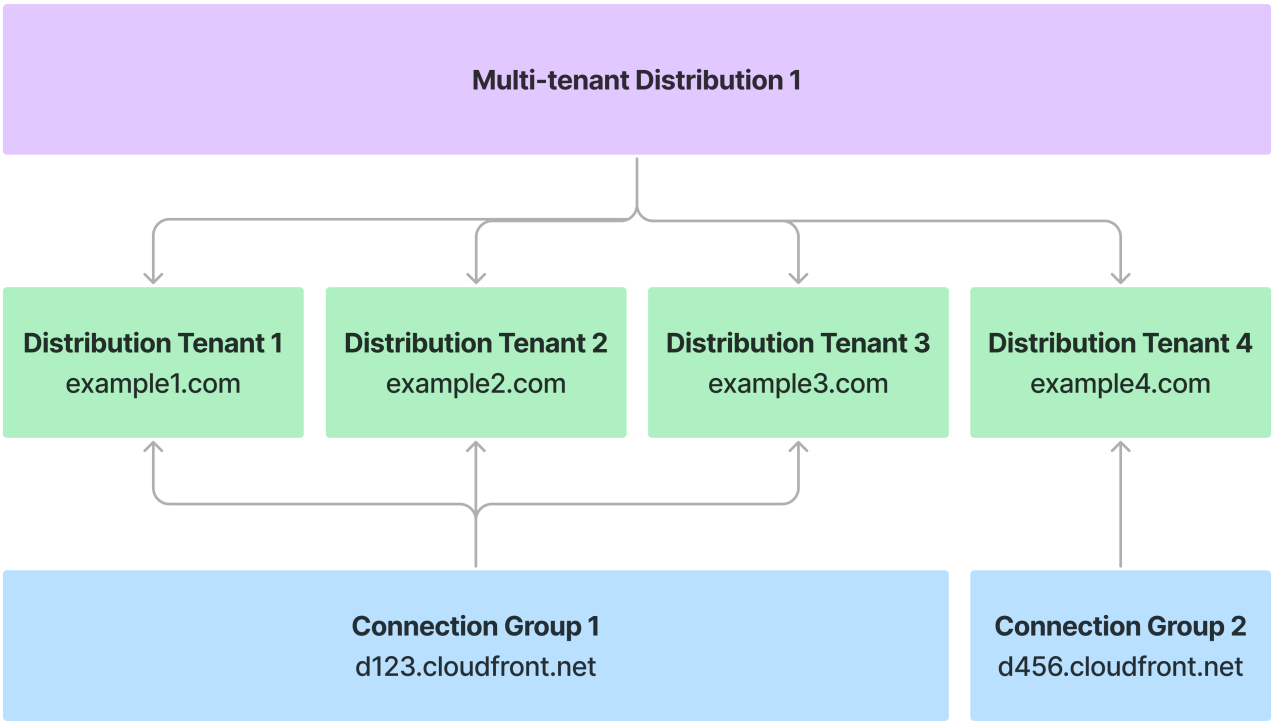
   Vous pouvez les modifier en créant manuellement un groupe de connexions. Pour plus d'informations, consultez Création d'un groupe de connexions personnalisé (facultatif).
3. Vous créez ensuite un ou plusieurs locataires de distribution. Le locataire de distribution constitue la « porte d'entrée » permettant aux utilisateurs d'accéder à votre contenu. Chaque tenant de distribution fait référence à la distribution multi-locataires et est automatiquement associé au groupe de connexion CloudFront créé pour vous. Le locataire de distribution prend en charge un domaine ou un sous-domaine individuel.
4. Vous pouvez ensuite personnaliser certains paramètres des locataires de distribution, tels que les domaines personnalisés et les chemins d'origine. Pour plus d'informations, consultez Personnalisations du locataire de distribution.
5. Enfin, vous devez mettre à jour l'enregistrement DNS de votre hôte DNS pour acheminer le trafic vers le locataire de distribution. Pour ce faire, récupérez la valeur du CloudFront point de terminaison auprès de votre groupe de connexion et créez un enregistrement CNAME pointant vers le CloudFront point de terminaison.

Example Exemple

Le graphique suivant illustre comment une distribution multi-locataires, des locataires de distribution et des groupes de connexions collaborent pour diffuser du contenu à vos utilisateurs sur plusieurs domaines.

1. La distribution multi-locataires définit les paramètres hérités pour chaque locataire de distribution. Vous utilisez la distribution multi-locataires comme modèle.
2. Chaque locataire de distribution créé à partir de la distribution multi-locataires possède son propre domaine.

3. Les locataires de distribution sont automatiquement ajoutés au groupe de connexion CloudFront créé pour vous lorsque vous avez créé la distribution multi-locataires. Les groupes de connexion contrôlent la manière dont les demandes des utilisateurs sont connectées au CloudFront réseau.



Pour obtenir des instructions détaillées sur la création d'une distribution multi-locataires, consultez Création d'une CloudFront distribution dans la console.

Termes

Les concepts suivants décrivent les composants des distributions multi-locataires :

Multi-tenant distribution

Un modèle de distribution multi-tenant qui spécifie tous les paramètres de configuration partagés pour tous les locataires de distribution, y compris le comportement du cache, les protections de sécurité et les origines. Multi-tenant les distributions ne peuvent pas desservir le trafic directement. Elles doivent donc être utilisées conjointement avec des groupes de connexions et des locataires de distribution.

Distribution standard

Une distribution qui ne dispose pas de fonctionnalités multi-locataires. Ces distributions sont idéales pour prendre en charge des sites web ou des applications uniques.

Locataire de distribution

Un locataire de distribution hérite de la configuration de distribution multi-locataires. Certains paramètres de configuration peuvent être personnalisés au niveau du locataire de distribution. Le locataire de distribution doit disposer d'un certificat TLS valide, qui peut être hérité de la distribution multi-locataires tant qu'il couvre le domaine ou le sous-domaine du locataire de distribution.

Le tenant de distribution doit être associé à un groupe de connexion. CloudFront crée un groupe de connexion pour vous lorsque vous créez un tenant de distribution, et assigne automatiquement tous les locataires de distribution à ce groupe de connexion.

Multi-tenancy

Vous pouvez utiliser la distribution multi-locataires pour diffuser du contenu sur plusieurs domaines, tout en partageant la configuration et l'infrastructure. Cette approche permet à différents domaines (appelés locataires) de partager des paramètres communs issus de la distribution multi-locataires, tout en conservant leurs propres personnalisations.

Groupe de connexions

Fournit le point CloudFront de terminaison de routage qui diffuse le contenu aux spectateurs. Vous devez associer chaque tenant de distribution à un groupe de connexion pour obtenir le point de terminaison de CloudFront routage correspondant à l'enregistrement CNAME que vous créez pour le domaine ou le sous-domaine de votre locataire de distribution. Les groupes de connexions peuvent être partagés entre plusieurs locataires de distribution. Les groupes de connexions gèrent les paramètres de routage pour les locataires de distribution, tels que les paramètres IPv6 et les listes d'adresses IP en unidiffusion.

Parameters

Liste de paires clé-valeur pour les valeurs d'espace réservé, telles que les chemins d'origine et les noms de domaine. Vous pouvez définir des paramètres dans votre distribution multi-locataires et fournir des valeurs pour ces paramètres au niveau du locataire de distribution. C'est vous qui décidez si les valeurs du paramètre doivent être saisies obligatoirement pour chaque locataire de distribution.

Si vous ne fournissez pas de valeur pour un paramètre facultatif dans un locataire de distribution, la valeur par défaut définie dans la distribution multi-locataires est utilisée.

CloudFront point final de routage

DNS canonique pour le groupe de connexions, tel que `d123.cloudfront.net`. Il est utilisé dans l'enregistrement CNAME de votre domaine ou sous-domaine de locataire de distribution.

Personnalisations

Vous pouvez personnaliser vos locataires de distribution afin qu'ils utilisent des paramètres différents de ceux de la distribution multi-locataires. Pour chaque locataire de distribution, vous pouvez spécifier une liste de contrôle d'accès AWS WAF Web (ACL), des certificats TLS et des restrictions géographiques différents.

Fonctions non prises en charge

Les fonctionnalités suivantes ne peuvent pas être utilisées avec une distribution multi-locataires. Si vous souhaitez créer une nouvelle distribution multi-locataires en utilisant les mêmes paramètres que votre distribution standard, notez que certains paramètres ne sont pas disponibles.

> **Remarques**
>
> - Actuellement, AWS Firewall Manager les politiques ne s'appliquent qu'à vos distributions standard. Firewall Manager ajoutera la prise en charge des distributions multi-locataires dans une future version.
> - Contrairement aux distributions standard, le nom de domaine (alias) doit être défini au niveau du locataire de distribution. Pour plus d'informations, consultez la section Demandez des certificats pour votre locataire CloudFront de distribution et le fonctionnement de l'CreateDistributionTenantAPI.

- Déploiement continu
- Identité d'accès d'origine (OAI) : utilisez plutôt le contrôle d'accès d'origine (OAC).
- Prise en charge SSL personnalisée avec IP dédiée : seule la méthode `sni-only` est prise en charge.
- AWS WAF ACL Web classique (V1) — Seules les ACL Web AWS WAF V2 sont prises en charge.

- Journalisation standard (héritée)
- TTL minimal
- TTL par défaut
- TTL maximal
- ForwardedValues
- PriceClass
- Signataires autorisés
- Smooth Streaming
- Gestion des identités et des accès AWS certificats de serveur (IAM)
- Adresses IP dédiées
- Version minimale du protocole SSLv3

Les paramètres suivants ne peuvent pas être configurés dans une distribution multi-locataires ou dans un locataire de distribution. Définissez plutôt les valeurs souhaitées dans un groupe de connexions. Tous les locataires de distribution associés au groupe de connexions utiliseront ces paramètres. Pour plus d'informations, consultez Création d'un groupe de connexions personnalisé (facultatif).

- Activation d'IPv6 (demandes des utilisateurs)
- Liste d'adresses IP statique en unidiffusion

Personnalisations du locataire de distribution

Lorsque vous utilisez une distribution multi-locataires, vos locataires de distribution héritent automatiquement de sa configuration. Cependant, vous pouvez personnaliser certains paramètres au niveau du locataire de distribution.

Vous pouvez personnaliser les éléments suivants :

- Paramètres : les paramètres sont des paires clé-valeur que vous pouvez utiliser pour le domaine d'origine ou les chemins d'origine. Consultez Fonctionnement des paramètres avec les locataires de distribution.
- AWS WAF ACL Web (V2) — Vous pouvez spécifier une ACL Web distincte pour le locataire de distribution, qui remplacera l'ACL Web utilisée pour la distribution multi-locataires. Vous pouvez

également désactiver ce paramètre pour un locataire de distribution spécifique, ce qui signifie que le locataire de distribution n'héritera pas des protections ACL web de la distribution multi-locataires. Pour plus d'informations, consultez AWS WAF ACL web.

- Restrictions géographiques : les restrictions géographiques que vous spécifiez pour un locataire de distribution remplaceront toutes les restrictions géographiques définies pour la distribution multi-locataires. Par exemple, si vous bloquez l'Allemagne (DE) dans votre distribution multi-locataires, tous les locataires de distribution associés bloqueront également DE. Toutefois, si vous autorisez DE pour un locataire de distribution spécifique, les paramètres de ce locataire remplaceront ceux de la distribution multi-locataires. Pour plus d'informations, consultez Restriction de la distribution géographique de votre contenu.
- Chemins d'invalidation : spécifiez les chemins de fichier vers le contenu que vous souhaitez invalider pour le locataire de distribution. Pour plus d'informations, consultez Invalidation de fichiers.
- Certificats TLS personnalisés : les certificats AWS Certificate Manager (ACM) que vous spécifiez pour les locataires de distribution complètent le certificat fourni dans la distribution multi-locataires. Cependant, si le même domaine est couvert à la fois par le certificat de la distribution multi-locataires et par celui du locataire de distribution, alors c'est le certificat du locataire qui est utilisé. Pour plus d'informations, consultez Demandez des certificats pour votre locataire CloudFront de distribution.
- Noms de domaine : vous devez spécifier au moins un nom de domaine par locataire de distribution.

Fonctionnement des paramètres avec les locataires de distribution

Un paramètre est une paire clé-valeur que vous pouvez utiliser comme valeur d'espace réservé. Définissez les paramètres que vous souhaitez utiliser dans votre distribution multi-locataires et précisez s'ils sont obligatoires.

Lorsque vous définissez des paramètres dans votre distribution multi-locataires, vous choisissez si ces paramètres doivent être renseignés au niveau du locataire de distribution.

- Si vous définissez les paramètres comme obligatoires dans la distribution multi-locataires, ils doivent alors être renseignés au niveau du locataire de distribution. (Ils ne sont pas hérités).
- Si les paramètres ne sont pas obligatoires, vous pouvez définir une valeur par défaut dans la distribution multi-locataires, laquelle sera héritée par le tenant de distribution.

Vous pouvez utiliser des paramètres dans les propriétés suivantes :

- Nom de domaine d'origine
- Chemin d'origine

Dans la distribution multi-locataires, vous pouvez définir jusqu'à deux paramètres pour chacune des propriétés précédentes.

Exemples de paramètres

Consultez les exemples suivants pour l'utilisation de paramètres pour le nom de domaine et le chemin d'origine.

Paramètres du nom de domaine

Dans la configuration de distribution multi-locataires, vous pouvez définir un paramètre pour le nom de domaine d'origine, comme dans les exemples suivants :

Amazon S3

- `{{parameter1}}.amzn-s3-demo-logging-bucket.s3.us-east-1.amazonaws.com`
- `{{parameter1}}-amzn-s3-demo-logging-bucket.s3.us-east-1.amazonaws.com`

Origines personnalisées

- `{{parameter1}}.lambda-url.us-east-1.on.aws`
- `{{parameter1}}.mediapackagev2.ap-south-1.amazonaws.com`

Lorsque vous créez un locataire de distribution, spécifiez la valeur à utiliser pour *parameter1*.

```
"Parameters": [
  {
    "Name": "parameter1",
    "Value": "mycompany-website"
  }
]
```

En utilisant les exemples précédemment définis dans la distribution multi-locataires, le nom de domaine d'origine du locataire de distribution se résout comme suit :

- *mycompany-website*`.amzn-s3-demo-bucket3.s3.us-east-1.amazonaws.com`

- *mycompany-website*-amzn-s3-demo-bucket3.s3.us-east-1.amazonaws.com
- *mycompany-website*.lambda-url.us-east-1.on.aws
- *mycompany-website*.mediapackagev2.ap-south-1.amazonaws.com

Paramètres du chemin d'origine

De la même manière, vous pouvez définir des paramètres pour le chemin d'origine dans la distribution multi-locataires, comme l'illustrent les exemples ci-dessous :

- /{{*parameter2*}}
- /{{*parameter2*}}/test
- /public/{{*parameter2*}}/test
- /search?name={{*parameter2*}}

Lorsque vous créez un locataire de distribution, spécifiez la valeur à utiliser pour *parameter2*.

```
"Parameters": [
  {
    "Name": "parameter2",
    "Value": "myBrand"
  }
]
```

En utilisant les exemples précédemment définis dans la distribution multi-locataires, le chemin d'origine du locataire de distribution se résout comme suit :

- /*myBrand*
- /*myBrand*/test
- /public/*myBrand*/test
- /search?name=*myBrand*

Example Exemple

Vous souhaitez créer plusieurs sites Web (locataires) pour vos clients, et vous devez vous assurer que chaque ressource de locataire de distribution utilise les valeurs correctes.

1. Vous créez une distribution multi-locataires et vous incluez deux paramètres pour la configuration du locataire de distribution.
2. Pour le nom de domaine d'origine, vous créez un paramètre nommé *customer-name* et spécifiez qu'il est obligatoire. Vous entrez le paramètre avant le compartiment S3, de sorte qu'il apparaisse comme suit :

   `{{customer-name}}.amzn-s3-demo-bucket3.s3.us-east-1.amazonaws.com`.
3. Pour le chemin d'origine, vous créez un deuxième paramètre nommé *my-theme* et spécifiez qu'il est facultatif, avec une valeur par défaut de*basic*. Votre chemin d'origine apparaît comme suit : `/{{my-theme}}`
4. Lorsque vous créez un locataire de distribution :
   - Pour le nom de domaine, vous devez spécifier une valeur pour*customer-name*, car elle est marquée comme obligatoire dans la distribution multi-locataires.
   - Pour le chemin d'origine, vous pouvez éventuellement spécifier une valeur *my-theme* ou utiliser la valeur par défaut.

Demandez des certificats pour votre locataire CloudFront de distribution

Lorsque vous créez un tenant de distribution, le locataire hérite du certificat partagé AWS Certificate Manager (ACM) de la distribution multi-locataires. Ce certificat partagé fournit le protocole HTTPS à tous les locataires associés à la distribution multi-locataires.

Lorsque vous créez ou mettez à jour un tenant de CloudFront distribution pour ajouter des domaines, vous pouvez ajouter un CloudFront certificat géré par ACM. CloudFront obtient ensuite un HTTP-validated certificat d'ACM en votre nom. Vous pouvez utiliser ce certificat ACM au niveau du locataire pour des configurations de domaine personnalisées. CloudFront rationalise le processus de renouvellement afin de maintenir les certificats à jour et de garantir la diffusion ininterrompue du contenu.

> **Note**
>
> Le certificat vous appartient, mais il ne peut être utilisé qu'avec CloudFront des ressources et la clé privée ne peut pas être exportée.

Vous pouvez demander le certificat lorsque vous créez ou mettez à jour le locataire de distribution.

Choisissez le mode de distribution des jetons de validation de certificat

Lorsque vous demandez un certificat géré pour un locataire de distribution via l'API ou la AWS CLI, spécifiez-le `ValidationTokenHost` dans`ManagedCertificateRequest`. Choisissez la valeur en fonction de la personne qui fournit le jeton de validation HTTP.

Les deux options demandent un certificat CloudFront-managed ACM. Le paramètre contrôle uniquement l'endroit où le jeton de validation est servi.

CloudFront-hosted (`cloudfront`)

> CloudFront sert automatiquement le jeton de validation HTTP. Choisissez cette option lorsque le domaine n'a aucun trafic existant ou lorsque vous pouvez pointer son DNS vers celui-ci CloudFront immédiatement.

Self-hosted (`self-hosted`)

> Vous diffusez le jeton de validation HTTP à partir de votre infrastructure existante. Choisissez cette option lorsque vous migrez un domaine avec du trafic existant. Le certificat peut être émis avant que vous ne pointiez le DNS vers CloudFront. Vous pouvez télécharger le fichier de jetons sur votre serveur existant ou configurer une redirection HTTP 301 (permanente) qui transmet les demandes de validation au point de terminaison de validation ACM.

Pour obtenir des instructions sur la finalisation de la configuration de la propriété du domaine, consultezConfiguration complète du domaine. Si vous le souhaitez`cloudfront`, sélectionnez Je n'ai pas de trafic. Si vous le souhaitez`self-hosted`, sélectionnez J'ai du trafic existant.

Pour plus d'informations sur les valeurs de l'API, consultez ManagedCertificateRequestla référence des CloudFront API.

Rubriques

- Ajout d’un domaine et d’un certificat (locataire de distribution)
- Configuration complète du domaine
- Pointer les domaines vers CloudFront
- Considérations relatives au domaine (locataire de distribution)
- Domaines génériques (locataire de distribution)

Ajout d’un domaine et d’un certificat (locataire de distribution)

La procédure suivante vous indique comment ajouter un domaine et mettre à jour le certificat d’un locataire de distribution.

Pour ajouter un domaine et un certificat (locataire de distribution)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans SaaS, choisissez Locataires de distribution.
3. Recherchez le locataire de distribution. Utilisez le menu déroulant de la barre de recherche pour filtrer par domaine, nom, ID de distribution, ID de certificat, ID de groupe de connexions ou ID de liste ACL web.
4. Choisissez le nom du locataire de distribution.
5. Pour domaines, choisissez Gérer le domaine.
6. Pour Certificat, choisissez si vous souhaitez utiliser un certificat TLS personnalisé pour votre locataire de distribution. Le certificat vérifie si vous êtes autorisé à utiliser le nom de domaine. Le certificat doit exister dans la région USA Est (Virginie du Nord).
7. Pour Domaines, choisissez Ajouter un domaine et entrez le domaine. En fonction de votre domaine, les messages suivants apparaîtront sous le nom de domaine que vous avez saisi.
   - Ce domaine est couvert par le certificat.
   - Ce domaine est couvert par le certificat, en attente de validation.
   - Ce domaine n’est pas couvert par le certificat. (Autrement dit, vous devez vérifier la propriété du domaine.)
8. Choisissez Mettre à jour le locataire de distribution.

   Sur la page des détails du locataire, sous Domaines, les champs suivants sont affichés :

   - Propriété du domaine : état de la propriété du domaine. Avant de CloudFront pouvoir diffuser du contenu, la propriété de votre domaine doit être vérifiée à l'aide de la validation du certificat TLS.
   - État du DNS : les enregistrements DNS de votre domaine doivent pointer CloudFront vers pour acheminer correctement le trafic.

9. Si la propriété de votre domaine n'est pas vérifiée, sur la page des détails du locataire, sous Domaines, sélectionnez Terminer la configuration du domaine, puis suivez la procédure suivante pour faire pointer l'enregistrement DNS vers votre nom de CloudFront domaine.

Configuration complète du domaine

Suivez ces procédures pour vérifier que vous êtes le propriétaire du domaine de vos locataires de distribution. Choisissez l'une des procédures suivantes en fonction de votre domaine.

> **Note**
>
> Si votre domaine est déjà pointé CloudFront par un enregistrement d'alias Amazon Route 53, vous devez ajouter votre enregistrement DNS TXT `_cf-challenge.` devant le nom de domaine. Cet enregistrement TXT vérifie que votre nom de domaine est lié à CloudFront. Répétez cette étape pour chaque domaine. L'exemple suivant montre comment mettre à jour votre enregistrement TXT :
>
> - Nom de l'enregistrement : `_cf-challenge.`*`DomainName`*
> - Type d'enregistrement : TXT
> - Valeur de l'enregistrement : *`CloudFrontRoutingEndpoint`*
>
> Votre enregistrement TXT pourrait, par exemple, se présenter ainsi : `_cf-challenge.example.com TXT d111111abcdef8.cloudfront.net`
> Vous pouvez trouver votre point de terminaison de CloudFront routage dans la console sur la page détaillée du locataire de distribution ou utiliser l'action ListConnectionGroupsAPI dans le Amazon CloudFront API Reference pour le trouver.

> **Tip**
>
> Si vous êtes un fournisseur de SaaS et que vous souhaitez autoriser l'émission de certificats sans obliger vos clients (locataires) à ajouter un enregistrement TXT directement à leur DNS, procédez comme suit :
>
> 1. Si vous êtes propriétaire du domaine `example-saas-provider.com`, attribuez des sous-domaines à vos locataires, tels que `customer-123.example-saas-provider.com`

2. Dans votre DNS, ajoutez l'enregistrement TXT `_cf-challenge.customer-123.example-saas-provider.com TXT d111111abcdef8.cloudfront.net` à votre configuration DNS.
3. Vos clients (les locataires) peuvent ensuite mettre à jour leur propre enregistrement DNS pour mapper leur nom de domaine au sous-domaine que vous avez fourni.

   ```
   www.customer-domain.com CNAME customer-123.example-saas-provider.com
   ```

I have existing traffic

Sélectionnez cette option si votre domaine ne tolère pas les durées d'indisponibilité. Vous devez avoir accès à votre origin/web serveur. Suivez la procédure suivante pour valider la propriété du domaine.

Pour terminer la configuration du domaine lorsque votre domaine reçoit déjà du trafic

1. Pour Spécifier votre trafic web, sélectionnez Mon domaine reçoit déjà du trafic, puis cliquez sur Suivant.
2. Pour Vérifier la propriété du domaine, choisissez l'une des options suivantes :

   - Utiliser un certificat existant : recherchez un certificat ACM existant ou entrez l'ARN du certificat qui couvre les domaines répertoriés.
   - Téléchargement manuel de fichiers : indiquez si vous pouvez téléverser des fichiers directement sur votre serveur web.

     Pour chaque domaine, créez un fichier en texte brut contenant votre jeton de validation à partir de l'emplacement du jeton, puis transférez-le vers votre origine à l'aide du Chemin de fichier spécifié sur votre serveur existant. Le chemin vers ce fichier peut ressembler à l'exemple suivant : `/.well-known/pki-validation/acm_9c2a7b2ec0524d09fa6013efb73ad123.txt`. Une fois cette étape terminée, ACM vérifie le jeton, puis émet le certificat TLS pour le domaine.
   - Redirection HTTP : choisissez cette option si vous n'avez pas d'accès direct pour télécharger des fichiers sur votre serveur web, ou si vous utilisez un CDN ou un service de proxy.

Pour chaque domaine, créez une redirection 301 sur votre serveur existant. Copiez le chemin well-known dans Rediriger depuis et pointez vers le point de terminaison du certificat spécifié dans Rediriger vers. Votre redirection peut ressembler à l'exemple suivant :

```
If the URL matches: example.com/.well-known/pki-validation/
leabe938a4fe077b31e1ff62b781c123.txt
Then the settings are:Forwarding URL
Then 301 Permanent Redirect:To validation.us-east-1.acm-
validations.aws/123456789012/.well-known/pki-validation/
leabe938a4fe077b31e1ff62b781c123.txt
```

> **Note**
>
> Vous pouvez choisir Vérifier l'état du certificat pour savoir à quel moment ACM émet le certificat pour le domaine.

3. Choisissez Suivant.
4. Terminez la procédure indiquée dans Pointer les domaines vers CloudFront.

I don't have traffic

Sélectionnez cette option si vous ajoutez de nouveaux domaines. CloudFront gérera la validation des certificats pour vous.

Pour terminer la configuration du domaine lorsque votre domaine ne reçoit pas encore de trafic

1. Pour Spécifier votre trafic web, choisissez Mon domaine ne reçoit pas encore de trafic.
2. Pour chaque nom de domaine, suivez la procédure indiquée dans Pointer les domaines vers CloudFront.
3. Après avoir mis à jour vos enregistrements DNS pour chaque nom de domaine, choisissez Suivant.
4. Patientez jusqu'à l'émission du certificat.

> **Note**
>
> Vous pouvez choisir Vérifier l'état du certificat pour savoir à quel moment ACM émet le certificat pour le domaine.

5. Sélectionnez Soumettre.

Pointer les domaines vers CloudFront

Mettez à jour vos enregistrements DNS pour acheminer le trafic de chaque domaine vers le point de terminaison CloudFront de routage. Vous pouvez utiliser plusieurs noms de domaine, mais ils doivent tous pointer vers ce point de terminaison.

Pour pointer des domaines vers CloudFront

1. Copiez la valeur du point CloudFront de terminaison de routage, telle que d111111abcdef8.cloudfront.net.
2. Mettez à jour vos enregistrements DNS pour acheminer le trafic de chaque domaine vers le point de terminaison CloudFront de routage.
    1. Connectez-vous à votre registre de domaine ou à la console de gestion de votre fournisseur DNS.
    2. Accédez à la section de gestion DNS correspondant à votre domaine.
        - Pour les sous-domaines : créez un enregistrement CNAME. Par exemple :
            - Nom : votre sous-domaine (tel que `www` ou `app`)
            - Value/Target — Le point de terminaison du CloudFront routage
            - Type d'enregistrement : CNAME
            - TTL : 3600 (ou ce qui convient à votre cas d'utilisation)
        - Pour les apex/root domaines : cela nécessite une configuration DNS unique, car les enregistrements CNAME standard ne peuvent pas être utilisés au niveau du domaine racine ou apex. Étant donné que la plupart des fournisseurs DNS ne prennent pas en charge les enregistrements ALIAS, nous vous recommandons de créer un enregistrement ALIAS dans Route 53. Par exemple :
            - Nom : votre domaine apex (tel que `example.com`)
            - Type d'enregistrement : A

- Alias : oui
- Alias cible : votre point de terminaison CloudFront de routage
- Stratégie de routage : Simple (ou selon ce qui convient à votre cas d'utilisation)

3. Vérifiez que la modification DNS s'est bien propagée. (Cela se produit généralement lorsque le TTL est expiré. Parfois, la propagation peut prendre de 24 à 48 heures.) Utilisez un outil tel que `dig` ou `nslookup`.

```
dig www.example.com
# Should eventually return a CNAME pointing to your CloudFront routing endpoint
```

3. Retournez à la CloudFront console et choisissez Soumettre. Lorsque votre domaine est actif, CloudFront met à jour le statut du domaine pour indiquer qu'il est prêt à recevoir du trafic.

Pour plus d'informations, consultez la documentation de votre fournisseur DNS :

- Cloudflare
- ClouDNS
- DNSimple
- Gandi.net
- GoDaddy
- Google Cloud DNS
- Nom : cheap

Considérations relatives au domaine (locataire de distribution)

Lorsqu'un domaine est actif, le contrôle du domaine a été établi et CloudFront répond à toutes les demandes des utilisateurs concernant ce domaine. Une fois activé, un domaine ne peut pas être désactivé ou remplacé par un état inactif. Le domaine ne peut pas être associé à une autre CloudFront ressource lorsqu'il est déjà utilisé. Pour associer le domaine à une autre distribution, utilisez la UpdateDomainAssociationdemande pour déplacer le domaine d'une CloudFront ressource à l'autre.

Lorsqu'un domaine est inactif, il CloudFront ne répond pas aux demandes des utilisateurs adressées au domaine. Si le domaine est inactif, tenez compte des éléments suivants :

- Si vous avez une demande de certificat en attente, CloudFront répondra aux demandes concernant le chemin connu. Tant que la demande est en attente, le domaine ne peut être associé à aucune autre CloudFront ressource.
- Si aucune demande de certificat n'est en attente, je CloudFront ne répondrai pas aux demandes concernant le domaine. Vous pouvez associer le domaine à d'autres CloudFront ressources.
- Vous ne pouvez avoir qu'une seule demande de certificat en attente par locataire de distribution. Pour demander un nouveau certificat couvrant d'autres domaines, vous devez d'abord annuler la demande en attente. L'annulation d'une demande de certificat existante ne supprime pas le certificat ACM associé. Vous pouvez le supprimer avec l'API ACM.
- Si vous appliquez un nouveau certificat à votre locataire de distribution, le certificat précédent sera dissocié. Vous pouvez réutiliser le certificat pour couvrir le domaine d'un autre locataire de distribution.

Comme pour les renouvellements de DNS-validated certificats, vous serez averti lorsque le renouvellement du certificat aboutira. Cependant, vous n'avez rien d'autre à faire. CloudFront gérera automatiquement le renouvellement des certificats pour votre domaine.

> **Note**
>
> Vous n'avez pas besoin d'appeler les opérations de l'API ACM pour créer ou mettre à jour vos ressources de certificats. Vous pouvez gérer vos certificats à l'aide des opérations CreateDistributionTenantet de UpdateDistributionTenantl'API pour spécifier les détails de votre demande de certificat géré.

> **Note**
>
> Compatibilité avec les restrictions géographiques : la validation des certificats CloudFront gérés est compatible avec les restrictions géographiques. Lorsque vous activez les restrictions géographiques sur une distribution qui utilise un certificat CloudFront géré, les demandes de validation sont exclues des règles de restriction géographique. Les autorités de certification vérifient la propriété du domaine à partir de plusieurs points de vue de réseaux répartis géographiquement (corroboration d'émission multiperspective) afin de se protéger contre le piratage BGP. CloudFront veille à ce que ces demandes de validation aboutissent, quels que soient les pays que vous bloquez ou autorisez.

Aucune action n'est requise pour utiliser cette fonctionnalité. Si vous avez précédemment supprimé les restrictions géographiques pour contourner les échecs de validation des certificats, vous pouvez les appliquer à nouveau en toute sécurité.

Domaines génériques (locataire de distribution)

Les domaines génériques sont pris en charge pour les locataires de distribution dans les situations suivantes :

- Lorsque le domaine générique figure dans le certificat partagé hérité de la distribution parente multi-locataires
- Lorsque vous utilisez un certificat TLS personnalisé valide pour votre locataire de distribution

Création d’un groupe de connexions personnalisé (facultatif)

Par défaut, CloudFront crée un groupe de connexion pour vous lorsque vous créez une distribution multi-locataires. Le groupe de connexion contrôle la manière dont les demandes de contenu des utilisateurs se connectent CloudFront.

Nous vous recommandons d’utiliser le groupe de connexions par défaut. Toutefois, si vous devez isoler des applications d’entreprise ou gérer des groupes de locataires de distribution séparément, vous pouvez choisir de créer un groupe de connexions personnalisé. Par exemple, vous devrez peut-être déplacer un locataire de distribution vers un groupe de connexions distinct s’il est victime d’une attaque DDoS. Ainsi, vous pouvez protéger les autres locataires de la distribution contre tout impact éventuel.

Création d’un groupe de connexions personnalisé (facultatif)

Vous pouvez éventuellement choisir de créer un groupe de connexions personnalisé pour vos locataires de distribution.

Pour créer un groupe de connexions personnalisé (facultatif)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Activez les paramètres du Groupe de connexions.

4. Dans le volet de navigation, choisissez Groupes de connexions, puis Créer un groupe de connexions.
5. Pour Nom du groupe de connexions, entrez un nom de groupe. Vous ne pouvez plus modifier ce nom une fois le groupe de connexions créé.
6. Pour IPv6, indiquez si vous souhaitez activer ce protocole IP. Pour plus d'informations, consultez Activation d'IPv6 (demandes des utilisateurs).
7. Pour la Liste d'adresses IP statiques en unidiffusion, indiquez si vous souhaitez acheminer du trafic vers vos locataires de distribution à partir d'un ensemble d'adresses IP. Pour plus d'informations, consultez Liste d'adresses IP statiques en unidiffusion.
8. (Facultatif) Ajoutez des balises à votre groupe de connexions.
9. Choisissez Créer un groupe de connexions.

Une fois le groupe de connexions créé, vous pourrez accéder aux paramètres configurés, à l'ARN et au point de terminaison.

- L'ARN ressemble à l'exemple suivant : `arn:aws:cloudfront::123456789012:connection-group/cg_2uVbA9KeWaADTbKzhj9lcKDoM25`
- Le point de terminaison ressemble à l'exemple suivant : d111111abcdef8.cloudfront.net

Vous pouvez modifier ou supprimer votre groupe de connexions personnalisé après l'avoir créé. Avant de supprimer un groupe de connexions, vous devez commencer par supprimer tous les locataires de distribution associés. Vous ne pouvez pas désactiver ou supprimer le groupe de connexion par défaut CloudFront créé pour vous lors de la création de votre distribution multi-locataires.

> **Important**
>
> Si vous modifiez le groupe de connexion d'un tenant de distribution, le trafic CloudFront continuera à être acheminé vers le tenant de distribution, mais avec une latence accrue. Nous vous recommandons de mettre à jour l'enregistrement DNS pour que le locataire de distribution utilise le point de terminaison de CloudFront routage du nouveau groupe de connexion.
>
> Jusqu'à ce que vous mettiez à jour l'enregistrement DNS, le routage CloudFront sera effectué en fonction des paramètres définis pour le point de terminaison de routage vers lequel le site Web pointe actuellement avec le DNS. Supposons que votre groupe de connexions par

défaut n'utilise pas d'adresses IP statiques en unidiffusion, alors que votre nouveau groupe de connexions personnalisé en utilise. Vous devez mettre à jour l'enregistrement DNS avant CloudFront d'utiliser les adresses IP statiques Anycast pour les locataires de distribution de votre groupe de connexion personnalisé.

Migration vers une distribution multi-locataires

Si vous disposez d'une distribution CloudFront standard et que vous souhaitez migrer vers une distribution multi-locataires, procédez comme suit.

Pour migrer d'une distribution standard vers une distribution multi-locataires

1. Prenez connaissance des Fonctions non prises en charge.
2. Créez une distribution multi-locataires avec la même configuration que votre distribution standard, à l'exception des fonctionnalités non prises en charge. Pour plus d'informations, consultez Création d'une CloudFront distribution dans la console.
3. Créez un locataire de distribution, puis ajoutez un autre nom de domaine dont vous êtes propriétaire.

   > **Warning**
   >
   > N'utilisez pas le nom de domaine actuel associé à votre distribution standard. Ajoutez plutôt un domaine fictif. Vous déplacerez votre domaine ultérieurement. Pour plus d'informations sur la création d'un locataire de distribution, consultez Création d'une CloudFront distribution dans la console.

4. Fournissez un certificat existant pour le domaine du locataire de distribution. Il s'agit du certificat qui couvrira le domaine fictif et le domaine que vous souhaitez déplacer.
5. Copiez le point de terminaison de CloudFront routage depuis la page détaillée du locataire de distribution dans la console. Vous pouvez également le trouver en utilisant l'action ListConnectionGroupsAPI dans le Amazon CloudFront API Reference.
6. Pour vérifier la propriété du domaine, créez un enregistrement DCV TXT avec un préfixe de soulignement (_) qui pointe vers le point de terminaison de CloudFront routage de votre locataire de distribution. Pour plus d'informations, consultez Pointer les domaines vers CloudFront.
7. Lorsque vos modifications se sont propagées, mettez à jour votre locataire de distribution afin qu'il utilise le domaine que vous avez précédemment utilisé pour votre distribution standard.

- Console : pour obtenir des instructions complètes, consultez Ajout d'un domaine et d'un certificat (locataire de distribution).
- API — Utilisez l'action UpdateDomainAssociationAPI dans le Amazon CloudFront API Reference.

> **Important**
>
> Cette action réinitialise la clé de cache de votre contenu. Ensuite, CloudFront commence à mettre en cache votre contenu à l'aide de la nouvelle clé de cache. Pour plus d'informations, consultez Comprendre la clé de cache.

8. Mettez à jour votre enregistrement DNS pour faire pointer votre domaine vers le point de terminaison de CloudFront routage de votre locataire de distribution. Une fois cette étape terminée, votre domaine sera prêt à envoyer du trafic à votre locataire de distribution. Pour plus d'informations, consultez Pointer les domaines vers CloudFront.
9. (Facultatif) Une fois que vous avez réussi à migrer votre domaine vers un locataire de distribution, vous pouvez utiliser un autre certificat CloudFront géré qui couvre le nom de domaine de votre locataire de distribution. Pour demander un certificat géré, créez un enregistrement TXT distinct pour émettre le certificat et suivez les étapes décrites dans Configuration complète du domaine.

Créer une distribution

Cette rubrique explique comment utiliser la CloudFront console pour créer une distribution.

Vue d'ensemble

1. Créez un ou plusieurs compartiments Amazon S3 ou configurez les serveurs HTTP en tant que serveurs d'origine. Une origine désigne l'emplacement où vous stockez la version originale de votre contenu. Lorsque CloudFront vous recevez une demande pour vos fichiers, elle est envoyée à l'origine pour récupérer les fichiers qu'elle distribue aux emplacements périphériques. Vous pouvez utiliser toute combinaison de compartiments Amazon S3 et de serveurs HTTP comme serveurs d'origine.

   - Si vous utilisez Amazon S3, le nom de votre compartiment doit être intégralement en lettres minuscules et ne peut pas contenir d'espaces.

- Si vous utilisez un serveur Amazon EC2 ou une autre origine personnalisée, consultez Utilisation d'Amazon EC2 (ou autre origine personnalisée).
- Pour connaître le nombre maximal actuel d'origines que vous pouvez créer pour une distribution ou pour demander un quota plus élevé, consultez Quotas généraux sur les distributions.

2. Téléchargez votre contenu sur vos serveurs d'origine. Vous rendez vos objets lisibles par le public ou vous pouvez utiliser des URL CloudFront signées pour restreindre l'accès à votre contenu.

   > **Important**
   >
   > Vous êtes responsable de la sécurité de votre serveur d'origine. Vous devez vous assurer qu'il CloudFront est autorisé à accéder au serveur et que les paramètres de sécurité protègent votre contenu.

3. Créez votre CloudFront distribution :

   - Pour une procédure détaillée de création d'une distribution dans la CloudFront console, consultezCréation d'une CloudFront distribution dans la console.
   - Pour plus d'informations sur la création d'une distribution à l'aide de l' CloudFront API, consultez CreateDistributionle Amazon CloudFront API Reference.

4. (Facultatif) Si vous utilisez la CloudFront console pour créer votre distribution, créez davantage de comportements de cache ou d'origines pour la distribution. Pour plus d'informations sur les comportements et les origines, consultez Pour mettre à jour une distribution multi-locataires.
5. Testez votre distribution. Pour plus d'informations sur les tests, consultez Test d'une distribution.
6. Développez votre site web ou votre application pour accéder à votre contenu à l'aide du nom de domaine renvoyé par CloudFront après la création de votre distribution à l'étape 3. Par exemple, si le nom de domaine de votre distribution est CloudFront renvoyé d111111abcdef8.cloudfront.net, l'URL du fichier dans un compartiment `image.jpg` Amazon S3 ou dans le répertoire racine d'un serveur HTTP est. `https://d111111abcdef8.cloudfront.net/image.jpg`

   Si vous avez spécifié un ou plusieurs noms de domaine alternatifs (CNAME) quand vous avez créé votre distribution, vous pouvez utiliser votre propre nom de domaine. Dans ce cas, l'URL de `image.jpg` pourrait être `https://www.example.com/image.jpg`.

   Remarques :

- Si vous voulez utiliser des URL signées pour limiter l'accès à votre contenu, consultez Offre de contenu privé avec des URL et des cookies signés.
- Si vous voulez livrer un contenu compressé, consultez Diffusion de fichiers compressés.
- Pour plus d'informations sur le comportement des CloudFront demandes et des réponses pour Amazon S3 et sur les origines personnalisées, consultezComportement des demandes et des réponses.

Rubriques

- Création d'une CloudFront distribution dans la console
- Valeurs CloudFront affichées dans la console
- Liens supplémentaires
- Ajoutez un domaine à votre distribution CloudFront standard

Création d'une CloudFront distribution dans la console

Lorsque vous créez une distribution, CloudFront configurez vos paramètres de distribution pour vous, en fonction du type d'origine de votre contenu. Pour en savoir plus sur les paramètres précédents, consultez Référence des paramètres de distribution préconfigurés. Vous pouvez également créer des distributions multi-locataires avec des paramètres qui peuvent être réutilisés entre plusieurs locataires de distribution. Pour plus d'informations, consultez Compréhension du fonctionnement des distributions multi-locataires. Vous pouvez également configurer manuellement vos propres paramètres de distribution.

Multi-tenant

Pour créer une distribution multi-locataires

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez Créer une distribution.
3. Choisissez Multi-tenant l'architecture, puis cliquez sur Suivant.
4. Entrez un Nom de distribution pour la distribution multi-locataires. Le nom s'affichera en tant que valeur de la clé `Name`. Cette valeur peut être modifiée par la suite. Vous pouvez ajouter

jusqu'à 50 balises pour votre distribution multi-locataires. Pour plus d'informations, consultez Marquer une CloudFront ressource.

5. (Facultatif) Pour le certificat Wildcard, choisissez le certificat AWS Certificate Manager (ACM) qui couvrira tous les sous-domaines du domaine racine, tels que. `*.example.com` Le certificat doit exister dans la région USA Est (Virginie du Nord).
6. Choisissez Suivant.
7. Sur la page Spécifier l'origine, sélectionnez le type d'origine à partir duquel votre contenu CloudFront sera extrait. CloudFront utilisera les paramètres recommandés pour ce type d'origine pour votre distribution multi-locataires. Pour plus d'informations sur les paramètres recommandés, consultez Référence des paramètres de distribution préconfigurés.
8. Pour Origine, sous le type d'origine sélectionné, sélectionnez ou renseignez l'origine que vous souhaitez utiliser.
9. Pour Chemin d'origine, entrez la barre oblique (`/`), suivie du chemin d'origine.
10. (Facultatif) Pour ajouter un paramètre, choisissez Insérer un paramètre pour le nom de domaine d'origine ou le chemin d'origine. Vous pouvez entrer jusqu'à deux paramètres par champ.

    a. Sélectionnez Créer un paramètre.

    b. Dans la boîte de dialogue Créer un paramètre, renseignez un nom unique dans Nom du paramètre et, si vous le souhaitez, une description.

    c. Pour Paramètre obligatoire, cochez la case afin de rendre cette valeur de paramètre obligatoire au niveau du locataire de distribution. S'il n'est pas obligatoire, saisissez une Valeur par défaut qui sera héritée par le locataire de distribution.

    d. Sélectionnez Create parameter (Créer un paramètre). Ce paramètre apparaît dans le champ correspondant.
11. Pour Options, choisissez l'une des options suivantes :

    - Utiliser les paramètres d'origine recommandés : utilisez les paramètres de cache et d'origine recommandés par défaut pour le type d'origine que vous avez sélectionné.
    - Personnaliser les paramètres d'origine : personnalisez le cache et les paramètres d'origine. Si vous choisissez cette option, indiquez vos propres valeurs qui s'afficheront.
12. Choisissez Suivant.
13. Sur la page Activer les protections de sécurité, choisissez si vous souhaitez activer les protections AWS WAF de sécurité. Vous pouvez, par la suite, personnaliser l'ACL web pour

des locataires de distribution spécifiques. Pour plus d'informations, consultez Enable AWS WAF pour une nouvelle distribution.

14. Choisissez Suivant, Créer une distribution.
15. Sur la page Distributions, votre distribution multi-locataires apparaît dans la liste des ressources. Le menu déroulant Toutes les distributions vous permet de filtrer vos distributions par type : standard ou multi-locataires. Vous pouvez également choisir la colonne Type pour filtrer vos distributions par type : standard ou multi-locataires.

Par défaut, CloudFront crée un groupe de connexion pour vous. Le groupe de connexion contrôle la manière dont les demandes de contenu des utilisateurs se connectent CloudFront. Vous pouvez personnaliser certains paramètres de routage dans le groupe de connexions. Pour plus d'informations, consultez Compréhension du fonctionnement des distributions multi-locataires.

Vous pouvez créer des locataires de distribution supplémentaires en utilisant la distribution multi-locataires comme modèle.

Pour créer un locataire de distribution

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, effectuez l'une des opérations suivantes :
   - Choisissez Distributions, choisissez une distribution multi-locataires, puis sélectionnez Créer un locataire.
   - Cliquez sur Locataires de distribution, puis choisissez Créer un locataire.
3. Dans Nom du locataire de distribution, entrez le nom souhaité. Le nom doit être unique dans votre nom Compte AWS et ne peut pas être modifié une fois que vous l'avez créé.
4. Pour Distribution modèle, choisissez un ID de distribution multi-locataires dans la liste.
5. Pour Gérer les balises, ajoutez jusqu'à 50 paires clé-valeur pour le locataire de distribution. Pour plus d'informations, consultez Marquer une CloudFront ressource.
6. Choisissez Suivant.
7. Sur la page Ajouter des domaines, pour Certificat, choisissez si vous souhaitez utiliser un Certificat TLS personnalisé pour votre locataire de distribution. Le certificat vérifie si vous êtes autorisé à utiliser le nom de domaine. Le certificat doit exister dans la région USA Est (Virginie du Nord).
8. Saisissez votre nom de votre domaine dans Domaines.

> **Note**
>
> Si vous avez saisi un nom de domaine qui n'est pas couvert par un certificat, vous devrez confirmer que vous en êtes le propriétaire. Vous pouvez tout de même créer le locataire de distribution pour le moment et vérifier la propriété du domaine ultérieurement. Pour plus d'informations, consultez Demandez des certificats pour votre locataire CloudFront de distribution.

9. Choisissez Suivant.
10. Les paramètres configurés dans la distribution multi-locataires sont affichés sur la page Définir les paramètres. Pour les paramètres obligatoires, entrez une valeur à côté du nom du paramètre et enregistrez vos modifications.
11. Pour ajouter un autre paramètre, choisissez Ajouter un paramètre, puis entrez un nom et une valeur.
12. Choisissez Suivant.
13. (Facultatif) Pour Personnalisation de la sécurité, si vous choisissez Remplacer les paramètres de distribution, sélectionnez l'option correspondant à votre cas d'utilisation.
14. (Facultatif) Dans Personnalisation des restrictions géographiques, si vous optez pour Remplacer les paramètres de distribution, choisissez le Type de restriction et les Pays appropriés pour le locataire de distribution. Pour plus d'informations, consultez Restriction de la distribution géographique de votre contenu.
15. Choisissez Suivant.
16. Choisissez Créer un locataire de distribution.

Tous vos locataires de distribution sont affichés sur la page Locataires de distribution. Vous pouvez appliquer un filtre sur les critères suivants :

Association

- ID de distribution
- ID de certificat
- ID du groupe de connexions
- ID d'ACL web

Propriétés

- Nom
- Domain

Vous pouvez modifier vos locataires de distribution afin de personnaliser des paramètres spécifiques. Pour plus d'informations, consultez Personnalisations du locataire de distribution.

Standard

Pour créer une distribution standard

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez Créer une distribution.
3. Entrez un Nom de distribution pour la distribution standard. Le nom sera affiché comme valeur pour la clé `Name` sous forme de balise. Cette valeur peut être modifiée par la suite. Vous pouvez ajouter jusqu'à 50 balises pour votre distribution standard. Pour plus d'informations, consultez Marquer une CloudFront ressource.
4. Choisissez Site web ou application unique, puis Suivant.
5. (Facultatif) Pour configurer un domaine, entrez un domaine déjà enregistré auprès de Route 53 dans votre Compte AWS domaine ou enregistrez un nouveau domaine. Suivez la procédure de configuration.

   - Si votre domaine utilise un fournisseur DNS autre que Route 53, vous pouvez toujours ajouter le domaine, mais cette étape devra être effectuée après la création de la distribution. Pour le moment, ignorez la configuration du domaine afin de poursuivre la création de la distribution. Vous devrez configurer manuellement le domaine et le certificat TLS ultérieurement. Pour plus d'informations, consultez Ajoutez un domaine à votre distribution CloudFront standard.
6. Choisissez Suivant.
7. Sur la page Spécifier l'origine, sélectionnez le type d'origine à partir duquel votre contenu CloudFront sera extrait. CloudFront utilisera les paramètres recommandés pour ce type d'origine pour votre distribution. Pour plus d'informations sur les paramètres recommandés, consultez Référence des paramètres de distribution préconfigurés.
8. Choisissez ou entrez votre origine dans Origine.

9. Dans Paramètres, choisissez l'une des options suivantes :

   - Utiliser les paramètres d'origine recommandés : utilisez les paramètres de cache et d'origine recommandés par défaut pour le type d'origine que vous avez sélectionné.
   - Personnaliser les paramètres d'origine : personnalisez le cache et les paramètres d'origine. Si vous choisissez cette option, renseignez vos propres valeurs.

10. Choisissez Suivant.
11. Sur la page Activer les protections de sécurité, choisissez si vous souhaitez activer les protections AWS WAF de sécurité.
12. Choisissez Suivant.
13. (Facultatif) Si vous utilisez Route 53 pour votre domaine, la page du certificat TLS s'affichera. Si vous ne CloudFront trouvez pas de certificat AWS Certificate Manager (ACM) existant pour votre domaine Compte AWS dans le `us-east-1` Région AWS, vous pouvez choisir de créer un certificat automatiquement ou de le créer manuellement. Une fois le certificat créé, choisissez Suivant.
14. Vérifiez les détails de votre distribution et choisissez Créer une distribution.
15. Après avoir CloudFront créé votre distribution, la valeur de la colonne État de votre distribution passera de Déploiement à la date et à l'heure de déploiement de la distribution.

    Le nom de domaine CloudFront attribué à votre distribution apparaît dans la liste des distributions. (Elle apparaît aussi sous l'onglet General d'une distribution sélectionnée.)

    > **Tip**
    >
    > Vous pouvez utiliser un autre nom de domaine au lieu du nom qui vous a été attribué par CloudFront, en suivant les étapes décrites dansUtilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME).

16. Lorsque votre distribution est déployée, vérifiez que vous pouvez accéder à votre contenu à l'aide de votre nouvelle CloudFront URL (d111111abcdef8.cloudfront.net) ou du CNAME. Pour plus d'informations, consultez Test d'une distribution.
17. Assurez-vous de mettre à jour vos enregistrements DNS pour indiquer le moment CloudFront où vous êtes prêt à envoyer du trafic vers votre distribution. Pour plus d'informations, consultez Pointer les domaines vers CloudFront (distribution standard).

Valeurs CloudFront affichées dans la console

Lorsque vous créez une nouvelle distribution ou que vous mettez à jour une distribution existante, CloudFront affiche les informations suivantes dans la CloudFront console.

> **Note**
>
> Les signataires fiables actifs, ceux Comptes AWS qui possèdent une paire de CloudFront clés active et peuvent être utilisés pour créer des URL signées valides, ne sont actuellement pas visibles dans la CloudFront console.

ID de distribution

Lorsque vous effectuez une action sur une distribution à l'aide de l' CloudFront API, vous utilisez l'ID de distribution pour spécifier la distribution à utiliser, par exemple`EDFDVBD6EXAMPLE`. Vous ne pouvez pas modifier l'ID d'une distribution.

Déploiement et état

Lorsque vous déployez une distribution, l'état du Déploiement s'affiche dans la colonne Dernière modification. Attendez que le déploiement de la distribution soit terminé et vérifiez que la colonne État indique Activé. Pour plus d'informations, consultez État de la distribution.

Dernière modification

Date et heure de dernière modification de la distribution, au format ISO 8601, par exemple le 19/05/2012T19:37:58Z. Pour plus d'informations, consultez https://www.w3.org/TR/NOTE-datetime.

Nom de domaine

Vous utilisez le nom de domaine de la distribution dans les liens vers vos objets. Par exemple, si le nom de domaine de votre distribution est `d111111abcdef8.cloudfront.net`, le lien vers `/images/image.jpg` sera `https://d111111abcdef8.cloudfront.net/images/image.jpg`. Vous ne pouvez pas modifier le nom de domaine CloudFront de votre distribution. Pour plus d'informations sur CloudFront les URL des liens vers vos objets, consultezPersonnalisez le format d'URL pour les fichiers dans CloudFront.

Si vous avez spécifié un ou plusieurs noms de domaine alternatifs (CNAME), vous pouvez utiliser vos propres noms de domaine pour les liens vers vos objets au lieu d'utiliser le nom de CloudFront domaine. Pour plus d'informations sur les CNAME, consultez Noms de domaine alternatifs (CNAME).

> **Note**
>
> CloudFront les noms de domaine sont uniques. Le nom de domaine de votre distribution n'avait jamais été utilisé pour une distribution précédente et ne sera jamais réutilisé pour une autre distribution à l'avenir.

Liens supplémentaires

Pour plus d'informations sur la création d'une distribution, consultez les liens suivants.

- Pour découvrir comment créer une distribution utilisant l'origine d'un compartiment Amazon Simple Storage Service (Amazon S3) avec un contrôle d'accès d'origine (OAC), consultez Commencez avec une distribution CloudFront standard.
- Pour plus d'informations sur l'utilisation des CloudFront API pour créer une distribution, consultez CreateDistributionle Amazon CloudFront API Reference.
- Pour en savoir plus sur la mise à jour d'une distribution (par exemple, pour ajouter des comportements de cache aux distributions standard ou pour personnaliser les locataires de distribution), consultez Mettre à jour une distribution.
- Pour afficher le nombre maximum actuel de distributions que vous pouvez créer pour chaque compte AWS ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas généraux sur les distributions.

Ajoutez un domaine à votre distribution CloudFront standard

Après avoir créé une nouvelle distribution CloudFront standard, vous pouvez y ajouter un domaine. Vous pouvez éventuellement configurer un domaine Amazon Route 53 pour votre distribution standard lors de sa création. Pour plus d'informations, consultez Création d'une CloudFront distribution dans la console.

Ajout d’un domaine à votre distribution standard existante

Pour ajouter un domaine à votre distribution standard

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis sélectionnez l’ID de distribution.
3. Dans Paramètres, Noms de domaine alternatifs, choisissez Ajouter un domaine.
4. Entrez jusqu’à cinq domaines à desservir.
5. Choisissez Suivant.
6. Pour le certificat TLS, si vous ne CloudFront trouvez pas de certificat AWS Certificate Manager (ACM) existant pour votre domaine Compte AWS dans le `us-east-1` Région AWS, vous pouvez en créer un.
   - Si vous utilisez Amazon Route 53 (Route 53), il crée CloudFront automatiquement un certificat pour vous.
7. Une fois votre certificat approvisionné, vous devez mettre à jour vos enregistrements DNS auprès de votre fournisseur DNS afin de prouver la propriété du domaine. Choisissez ensuite Valider le certificat. Pour plus d’informations, consultez Pointer les domaines vers CloudFront (distribution standard).
   - Si vous utilisez Route 53, mettez CloudFront à jour vos enregistrements DNS pour vous.
8. Choisissez Suivant.
9. Passez en revue vos modifications et choisissez Ajouter des domaines.
10. Avant d'envoyer du trafic vers votre distribution, assurez-vous de mettre à jour vos enregistrements DNS pour qu'ils pointent vers CloudFront. Pour plus d'informations, choisissez Router les domaines vers CloudFront dans la section Paramètres de la page des détails de votre distribution.
    - Si vous utilisez Route 53, vous pouvez avoir CloudFront configuré automatiquement le routage DNS pour vous.

Pointer les domaines vers CloudFront (distribution standard)

Mettez à jour vos enregistrements DNS pour acheminer le trafic de chaque domaine vers le CloudFront nom d'hôte. Vous pouvez utiliser plusieurs noms de domaine, mais ils doivent tous pointer vers ce nom d’hôte.

Pour pointer des domaines vers CloudFront

1. Copiez la valeur du CloudFront nom d'hôte, par exemple d111111abcdef8.cloudfront.net.
2. Mettez à jour vos enregistrements DNS pour acheminer le trafic de chaque domaine vers le CloudFront nom d'hôte.
    1. Connectez-vous à votre registre de domaine ou à la console de gestion de votre fournisseur DNS.
    2. Accédez à la section de gestion DNS correspondant à votre domaine.
        - Pour les sous-domaines : créez un enregistrement CNAME. Par exemple :
            - Nom : votre sous-domaine (tel que `www` ou `app`)
            - Valeur/ Cible — Votre nom CloudFront d'hôte
            - Type d’enregistrement : CNAME
            - TTL : 3600 (ou ce qui convient à votre cas d’utilisation)
        - Pour les apex/root domaines : cela nécessite une configuration DNS unique, car les enregistrements CNAME standard ne peuvent pas être utilisés au niveau du domaine racine ou apex. Étant donné que la plupart des fournisseurs DNS ne prennent pas en charge les enregistrements ALIAS, nous vous recommandons de créer un enregistrement ALIAS dans Route 53. Par exemple :
            - Nom : votre domaine apex (tel que `example.com`)
            - Type d’enregistrement : A
            - Alias : oui
            - Alias cible : votre nom CloudFront d'hôte
            - Stratégie de routage : Simple (ou selon ce qui convient à votre cas d’utilisation)
    3. Vérifiez que la modification DNS s’est bien propagée. (Cela se produit généralement lorsque le TTL est expiré. Parfois, la propagation peut prendre de 24 à 48 heures.) Utilisez un outil tel que `dig` ou `nslookup`.

        ```
        dig www.example.com
        ```

```
# Should eventually return a CNAME pointing to your CloudFront hostname
```

3. Retournez à la CloudFront console et choisissez Soumettre. Lorsque votre domaine est actif, CloudFront met à jour le statut du domaine pour indiquer qu'il est prêt à recevoir du trafic.

Pour plus d’informations, consultez la documentation de votre fournisseur DNS :

- Cloudflare
- ClouDNS
- DNSimple
- Gandi.net
- GoDaddy
- Google Cloud DNS
- Nom : cheap

Référence des paramètres de distribution préconfigurés

Lorsque vous créez votre CloudFront distribution, configure CloudFront automatiquement la plupart des paramètres de distribution pour vous, en fonction du type d'origine de votre contenu. Vous pouvez, si vous le souhaitez, modifier manuellement les paramètres de votre distribution. Pour plus d’informations, consultez Référence de tous les paramètres de distribution.

Les sections suivantes décrivent les paramètres de préconfiguration par défaut pour les distributions, ainsi que les paramètres que vous pouvez personnaliser.

Origine Amazon S3

Vous trouverez ci-dessous les paramètres d'origine CloudFront préconfigurés pour votre origine Amazon S3 dans une distribution multi-locataires.

Paramètres d’origine (préconfigurés)

- Origin Access Control (console uniquement) : CloudFront configurez cela pour vous. CloudFront tente d'ajouter la politique de compartiment S3 pour les distributions standard et pour les distributions multi-locataires sans qu'aucun paramètre ne soit utilisé dans le domaine d'origine.
- Ajouter un en-tête personnalisé : aucun
- Activer Origin Shield : non

- Tentatives de connexion : 3

Vous trouverez ci-dessous les paramètres de cache CloudFront préconfigurés pour votre origine Amazon S3 dans une distribution multi-locataires.

Paramètres de mise en cache (préconfigurés)

- Compresser des objets automatiquement : oui
- Politique du protocole utilisateur : redirection vers HTTPS
- Méthodes HTTP autorisées : `GET, HEAD`
- Limiter l'accès utilisateur : non
- Politique de cache : `CachingOptimized`
- Politique de demande d'origine : aucune
- Politique d'en-tête de réponse : aucune
- Smooth Streaming : non
- Chiffrement au niveau du champ : non
- Activer les journaux d'accès en temps réel — Non
- Fonctions : non

Voici les paramètres que vous pouvez personnaliser pour votre origine Amazon S3 dans une distribution multi-locataires.

Paramètres personnalisables

- Accès S3 : CloudFront définit cela pour vous, en fonction des paramètres de votre compartiment S3 :
  - Si votre compartiment est public : aucune politique de contrôle d'accès d'origine (OAC) n'est requise.
  - Si votre compartiment est privé : vous pouvez sélectionner ou créer une politique OAC à utiliser.
- Activer Origin Shield : non
- Compresser des objets automatiquement : oui
  - Si vous choisissez Oui, la politique de mise en cache `CachingOptimized` est utilisée.
  - Si vous choisissez Non, la politique de mise en cache `CachingOptimizedForUncompressedObjects` est utilisée.

Origine API Gateway

Vous trouverez ci-dessous les paramètres d'origine CloudFront préconfigurés pour votre origine API Gateway dans une distribution multi-locataires.

Paramètres d’origine (préconfigurés)

- Protocole : HTTPS uniquement
- Port HTTPS : 443
- Protocole SSL d'origine minimal — TLSv1.2
- Chemin d’origine : aucun
- Origin Access Control (console uniquement) : CloudFront configurez cela pour vous
- Ajouter un en-tête personnalisé : aucun
- Activer Origin Shield : non
- Tentatives de connexion : 3
- Délai de réponse : 30
- Keep-alive délai d'expiration — 5

Vous trouverez ci-dessous les paramètres de cache qui sont CloudFront préconfigurés pour votre origine API Gateway dans une distribution multi-locataires.

Paramètres de mise en cache (préconfigurés)

- Compresser des objets automatiquement : oui
- Politique du protocole utilisateur : redirection vers HTTPS
- Méthodes HTTP autorisées : `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Méthodes HTTP de mise en cache : non
- Autoriser les requêtes gRPC au-delà de la limite — HTTP/2 Non
- Limiter l’accès utilisateur : non
- Politique de cache : `CachingDisabled` (valeurs possibles : `UseOriginCacheControlHeaders`, `UseOriginCacheControlHeaders-QueryStrings`)
- Politique de demande d’origine : `AllViewerExceptHostHeader` (valeurs possibles : `AllViewer`, `AllViewerandCloudFrontHeaders-2022-06`)

- Politique d’en-tête de réponse : aucune
- Smooth Streaming : non
- Chiffrement au niveau du champ : non
- Activer les journaux d'accès en temps réel — Non
- Fonctions : non

Voici les paramètres que vous pouvez personnaliser pour votre origine API Gateway dans une distribution multi-locataires.

Paramètres personnalisables

- Activer Origin Shield : (par défaut : non)
- Compresser les objets automatiquement : (par défaut : oui)

Origine personnalisée et instance EC2

Vous trouverez ci-dessous les paramètres d'origine CloudFront préconfigurés pour votre origine personnalisée dans une distribution multi-locataires.

Paramètres d’origine (préconfigurés)

- Protocole : utiliser le même protocole que l’utilisateur
- Port HTTP : 80
- Port HTTPS : 443
- Protocole SSL d'origine minimal — TLSv1.2
- Chemin d’origine : aucun
- Ajouter un en-tête personnalisé : aucun
- Activer Origin Shield : non
- Tentatives de connexion : 3
- Délai de réponse : 30
- Keep-alive délai d'expiration — 5

Vous trouverez ci-dessous les paramètres de cache qui sont CloudFront préconfigurés pour votre origine personnalisée et votre instance EC2 dans une distribution multi-locataires.

Paramètres de mise en cache (préconfigurés)

- Compresser des objets automatiquement : oui
- Politique du protocole utilisateur : redirection vers HTTPS
- Méthodes HTTP autorisées : `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Méthodes HTTP de mise en cache : non
- Autoriser les requêtes gRPC au-delà de la limite — HTTP/2 Non
- Limiter l'accès utilisateur : non
- Politique de cache : `UseOriginCacheControlHeaders` (valeurs possibles : `UseOriginCacheControlHeaders-QueryStrings`, `CachingDisabled`, `CacheOptimized`, `CachingOptimizedForUncompressedObjects`)
- Politique de demande d'origine : `AllViewer` (valeurs possibles : `AllViewerExceptHostHeader`, `AllViewerandCloudFrontHeaders-2022-06`)
- Politique d'en-tête de réponse : aucune
- Smooth Streaming : non
- Chiffrement au niveau du champ : non
- Activer les journaux d'accès en temps réel — Non
- Fonctions : non

Voici les paramètres que vous pouvez personnaliser pour votre origine personnalisée et votre instance EC2 dans une distribution multi-locataires.

Paramètres personnalisables

- Activer Origin Shield : (par défaut : non)
- Compresser les objets automatiquement : (par défaut : oui)
- Mise en cache : (par défaut : `Cache by Default`)
  - Si l'option `Cache by Default` est sélectionnée, la politique de cache `UseOriginCacheControlHeaders` est utilisée.
  - Si l'option `Do Not Cache by Default` est sélectionnée, la politique de cache `CachingDisabled` est utilisée.
- Inclure la chaîne de requête dans le cache : (par défaut : oui, si l'option `Cache by Default` est déjà sélectionnée)

- Si l’option `Do Not Cache by Default` est déjà sélectionnée et que vous choisissez ensuite d’inclure la chaîne de requête dans le cache, la politique de cache `UseOriginCacheControlHeaders-QueryStrings` est utilisée.

origine Elastic Load Balancing

Vous trouverez ci-dessous les paramètres d'origine CloudFront préconfigurés pour votre origine Elastic Load Balancing dans une distribution multi-locataires.

Paramètres d’origine (préconfigurés)

- Protocole : HTTPS uniquement
- Port HTTPS : 443
- Protocole SSL d'origine minimal — TLSv1.2
- Chemin d’origine : aucun
- Ajouter un en-tête personnalisé : aucun
- Activer Origin Shield : non
- Tentatives de connexion : 3
- Délai de réponse : 30
- Keep-alive délai d'expiration — 5

Vous trouverez ci-dessous les paramètres de cache CloudFront préconfigurés pour votre origine Elastic Load Balancing dans une distribution multi-locataires.

Paramètres de mise en cache (préconfigurés)

- Compresser des objets automatiquement : oui
- Politique du protocole utilisateur : redirection vers HTTPS
- Méthodes HTTP autorisées : `GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE`
- Méthodes HTTP de mise en cache : non
- Autoriser les requêtes gRPC au-delà de la limite — HTTP/2 Non
- Limiter l’accès utilisateur : non
- Mise en cache : (par défaut : `Cache by Default`)

  - Si l'option `Cache by Default` est sélectionnée, la politique de cache `UseOriginCacheControlHeaders` est utilisée.
  - Si l'option `Do Not Cache by Default` est sélectionnée, la politique de cache `CachingDisabled` est utilisée.
- Inclure la chaîne de requête dans le cache : (par défaut : oui, si l'option `Cache by Default` est déjà sélectionnée)
  - Si l'option `Do Not Cache by Default` est déjà sélectionnée et que vous choisissez ensuite d'inclure la chaîne de requête dans le cache, la politique de cache `UseOriginCacheControlHeaders-QueryStrings` est utilisée.
- Politique de demande d'origine : `All Viewer` (valeurs possibles : `AllViewerExceptHostHeader`, `AllViewerandCloudFrontHeaders-2022-06`)
- Politique d'en-tête de réponse : aucune
- Smooth Streaming : non
- Chiffrement au niveau du champ : non
- Activer les journaux d'accès en temps réel — Non
- Fonctions : non

Voici les paramètres que vous pouvez personnaliser pour votre origine Elastic Load Balancing dans une distribution multi-locataires.

Paramètres personnalisables

- Activer Origin Shield : (par défaut : non)
- Compresser les objets automatiquement : (par défaut : oui)
- Mise en cache : (par défaut : `Cache by Default`)
  - Si l'option `Cache by Default` est sélectionnée, la politique de cache `UseOriginCacheControlHeaders` est utilisée.
  - Si l'option `Do Not Cache by Default` est sélectionnée, la politique de cache `CachingDisabled` est utilisée.
- Inclure la chaîne de requête dans le cache : (par défaut : oui, si l'option `Cache by Default` est déjà sélectionnée)
  - Si l'option `Do Not Cache by Default` est déjà sélectionnée et que vous choisissez ensuite d'inclure la chaîne de requête dans le cache, la politique de cache `UseOriginCacheControlHeaders-QueryStrings` est utilisée.

MediaPackage origine v1

Vous trouverez ci-dessous les paramètres d'origine CloudFront préconfigurés pour votre origine MediaPackage v1 dans une distribution multi-locataires.

Paramètres d’origine (préconfigurés)

- Protocole : HTTPS uniquement
- Port HTTPS : 443
- Protocole SSL d'origine minimal — TLSv1.2
- Chemin d'origine : vous le fournissez en saisissant votre MediaPackage URL.
- Ajouter un en-tête personnalisé : aucun
- Activer Origin Shield : non
- Tentatives de connexion : 3
- Délai de réponse : 30
- Keep-alive délai d'expiration — 5

Vous trouverez ci-dessous les paramètres de cache qui sont CloudFront préconfigurés pour votre origine MediaPackage v1 dans une distribution multi-locataires.

Paramètres de mise en cache (préconfigurés)

- Compresser des objets automatiquement : oui
- Politique du protocole utilisateur : redirection vers HTTPS
- Méthodes HTTP autorisées : `GET, HEAD`
- Méthodes HTTP de mise en cache : non
- Autoriser les requêtes gRPC au-delà de la limite — HTTP/2 Non
- Limiter l’accès utilisateur : non
- Politique de cache : `Elemental-MediaPackage`
- Politique de demande d’origine : aucune
- Politique d’en-tête de réponse : aucune
- Smooth Streaming : non
- Chiffrement au niveau du champ : non

- Activer les journaux d'accès en temps réel — Non
- Fonctions : non

MediaPackage origine v2

Vous trouverez ci-dessous les paramètres d'origine CloudFront préconfigurés pour votre origine MediaPackage v2 dans une distribution multi-locataires.

Paramètres d’origine (préconfigurés)

- Origin Access Control : CloudFront configure cela pour vous et ajoute la politique
- Protocole : HTTPS uniquement
- Port HTTPS : 443
- Protocole SSL d'origine minimal — TLSv1.2
- Chemin d’origine : aucun
- Ajouter un en-tête personnalisé : aucun
- Activer Origin Shield : non
- Tentatives de connexion : 3
- Délai de réponse : 30
- Keep-alive délai d'expiration — 5

Vous trouverez ci-dessous les paramètres de cache qui sont CloudFront préconfigurés pour votre origine MediaPackage v2 dans une distribution multi-locataires.

Paramètres de mise en cache (préconfigurés)

- Compresser des objets automatiquement : oui
- Politique du protocole utilisateur : redirection vers HTTPS
- Méthodes HTTP autorisées : `GET, HEAD`
- Méthodes HTTP de mise en cache : non
- Autoriser les requêtes gRPC au-delà de la limite — HTTP/2 Non
- Limiter l’accès utilisateur : non
- Politique de cache : `Elemental-MediaPackage`

- Politique de demande d’origine : aucune
- Politique d’en-tête de réponse : aucune
- Smooth Streaming : non
- Chiffrement au niveau du champ : non
- Activer les journaux d'accès en temps réel — Non
- Fonctions : non

MediaTailor origine

Vous trouverez ci-dessous les paramètres d'origine CloudFront préconfigurés pour votre MediaTailor origine dans une distribution multi-locataires.

Paramètres d’origine (préconfigurés)

- Protocole : HTTPS uniquement
- Port HTTPS : 443
- Protocole SSL d'origine minimal — TLSv1.2
- Chemin d'origine : vous le fournissez en saisissant votre MediaPackage URL.
- Ajouter un en-tête personnalisé : aucun
- Activer Origin Shield : non
- Tentatives de connexion : 3
- Délai de réponse : 30
- Keep-alive délai d'expiration — 5

Vous trouverez ci-dessous les paramètres de cache qui sont CloudFront préconfigurés pour votre MediaTailor origine dans une distribution multi-locataires.

Paramètres de mise en cache (préconfigurés)

- Compresser des objets automatiquement : oui
- Politique du protocole utilisateur : redirection vers HTTPS
- Méthodes HTTP autorisées : `GET, HEAD`
- Méthodes HTTP de mise en cache : non

- Autoriser les requêtes gRPC au-delà de la limite — HTTP/2 Non
- Limiter l'accès utilisateur : non
- Politique de cache : aucune
- Politique de demande d'origine : `Elemental-MediaTailor-PersonalizedManifests`
- Politique d'en-tête de réponse : aucune
- Smooth Streaming : non
- Chiffrement au niveau du champ : non
- Activer les journaux d'accès en temps réel — Non
- Fonctions : non

Référence de tous les paramètres de distribution

Vous pouvez choisir de modifier manuellement vos paramètres CloudFront de distribution lorsque vous créez ou mettez à jour votre distribution. Vous pouvez modifier les paramètres suivants :

CloudFront Configure toutefois la plupart des paramètres de distribution pour vous, en fonction du type d'origine de votre contenu. Pour plus d'informations, consultez Référence des paramètres de distribution préconfigurés.

Pour de plus amples informations sur la création ou la mise à jour d'une distribution à l'aide de la console CloudFront, veuillez consulter the section called "Créer une distribution" ou the section called "Mettre à jour une distribution".

Rubriques

- Paramètres d'origine
- Paramètres de comportement du cache
- Paramètres de distribution
- Pages d'erreur personnalisées et mise en cache des erreurs
- Restrictions géographiques

Paramètres d'origine

Lorsque vous utilisez la CloudFront console pour créer ou mettre à jour une distribution, vous fournissez des informations sur un ou plusieurs emplacements, appelés origines, où vous stockez

les versions originales de votre contenu Web. CloudFront récupère votre contenu Web depuis vos origines et le diffuse aux spectateurs à l'aide d'un réseau mondial de serveurs périphériques.

Pour connaître le nombre maximal actuel d'origines que vous pouvez créer pour une distribution ou pour demander un quota plus élevé, consultez the section called "Quotas généraux sur les distributions".

Si vous voulez supprimer une origine, vous devez d'abord modifier ou supprimer les comportements de cache associés à cette origine.

> **Important**
>
> Si vous supprimez une origine, confirmez que les fichiers qui étaient précédemment remis par cette origine sont disponibles dans une autre origine et que vos comportements de cache acheminent désormais ces fichiers vers la nouvelle origine.

Lorsque vous créez ou mettez à jour une distribution web, vous spécifiez les valeurs suivantes pour chaque origine.

Rubriques

- Domaine d'origine
- Protocole (origines personnalisées uniquement)
- Chemin d'origine
- Nom
- Accès à l'origine (origines Amazon S3 uniquement)
- Ajout d'en-tête personnalisé
- Activer Origin Shield
- Tentatives de connexion
- Délai de connexion
- Délai de réponse
- Délai d'exécution de la réponse
- Keep-alive délai d'expiration (origines personnalisées et VPC uniquement)
- Quotas de délai de réponse et d'attente des connexions actives

Domaine d'origine

Le domaine d'origine est le nom de domaine DNS de la ressource où CloudFront seront obtenus les objets correspondant à votre origine, tels qu'un bucket Amazon S3 ou un serveur HTTP. Par exemple :

- Compartiment Amazon S3 : *amzn-s3-demo-bucket*.s3.*us-west-2*.amazonaws.com

> **Note**
>
> Si vous avez récemment créé le compartiment S3, la CloudFront distribution peut renvoyer `HTTP 307 Temporary Redirect` des réponses pendant 24 heures au maximum. La propagation du nom du compartiment S3 à toutes les régions AWS peut prendre jusqu'à 24 heures. Lorsque la propagation est terminée, la distribution arrête automatiquement l'envoi de ces réponses de redirection ; vous n'avez pas besoin de prendre d'action. Pour plus d'informations, consultez Pourquoi Amazon S3 m'envoie-t-il une réponse de redirection temporaire HTTP 307 ? et Redirection de demande temporaire.

- Compartiment Amazon S3 configuré en tant que site web : *amzn-s3-demo-bucket*.s3-website.*us-west-2*.amazonaws.com
- MediaStore contenant — *examplemediastore*.data.mediastore.*us-west-1*.amazonaws.com
- MediaPackage point de terminaison — *examplemediapackage*.mediapackage.*us-west-1*.amazonaws.com
- Instance Amazon EC2 : *ec2-203-0-113-25*.compute-1.amazonaws.com
- Équilibreur de charge Elastic Load Balancing : *example-load-balancer-1234567890*.*us-west-2*.elb.amazonaws.com
- Votre propre serveur web : www.example.com

Choisissez le nom de domaine dans le champ Domaine d'origine ou saisissez le nom. Les ressources provenant des régions d'adhésion doivent être saisies manuellement. Le nom de domaine n'est pas sensible à la casse. Votre domaine d'origine doit avoir un nom DNS publiquement résolu qui achemine les demandes des clients vers les cibles via Internet.

Si vous configurez CloudFront pour vous connecter à votre origine via HTTPS, l'un des noms de domaine du certificat doit correspondre au nom de domaine que vous avez spécifié pour le nom

de domaine d'origine. Si aucun nom de domaine ne correspond, CloudFront renvoie le code d'état HTTP 502 (Bad Gateway) au lecteur. Pour plus d'informations, consultez Noms de domaine dans la CloudFront distribution et dans le certificat et SSL/TLS échec de négociation entre CloudFront et un serveur d'origine personnalisé.

> **Note**
>
> Si vous utilisez une politique de demande d'origine qui transfère l'en-tête d'hôte de l'utilisateur à l'origine, celle-ci doit répondre avec un certificat correspondant à cet en-tête d'hôte. Pour plus d'informations, consultez Ajouter des en-têtes de CloudFront demande.

Si votre origine est un compartiment Amazon S3, notez les points suivants :

- Si le compartiment est configuré comme site web, entrez le point de terminaison de l'hébergement du site web statique Amazon S3 de votre compartiment ; ne sélectionnez pas le nom du compartiment dans la liste du champ Origin domain (Domaine d'origine). Le point de terminaison de l'hébergement du site web statique s'affiche dans la console Amazon S3, sur la page Properties (Propriétés) sous Static Website Hosting (Hébergement de site Web statique). Pour plus d'informations, consultez the section called "Utilisation d'un compartiment Amazon S3 configuré en tant que point de terminaison de site web".
- Si vous avez configuré Amazon S3 Transfer Acceleration pour votre compartiment, ne spécifiez pas le point de terminaison `s3-accelerate` pour Origin domain (Domaine d'origine).
- Si vous utilisez un bucket provenant d'un autre AWS compte et si le bucket n'est pas configuré en tant que site Web, entrez le nom au format suivant :

  `bucket-name``.s3.`*`region`*`.amazonaws.com`

  Si votre compartiment se trouve dans la région USA et que vous voulez qu'Amazon S3 route les demandes vers une installation située en Virginie du Nord, utilisez le format suivant :

  `bucket-name``.s3.us-east-1.amazonaws.com`
- Les fichiers doivent être lisibles par le public, sauf si vous sécurisez votre contenu dans Amazon S3 à l'aide d'un contrôle CloudFront d'accès à l'origine. Pour plus d'informations sur le contrôle d'accès, consultez the section called "Restriction de l'accès à une origine Amazon S3".

> **Important**
>
> Si l'origine est un compartiment Amazon S3, le nom du compartiment doit être conforme aux exigences de dénomination DNS. Pour plus d'informations, consultez Limites et restrictions applicables aux compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

Lorsque vous modifiez la valeur du domaine d'origine pour une origine, commence CloudFront immédiatement à répliquer la modification aux emplacements CloudFront périphériques. Jusqu'à ce que la configuration de distribution soit mise à jour dans un emplacement périphérique donné, CloudFront continue de transférer les demandes vers l'origine précédente. Dès que la configuration de distribution est mise à jour dans cet emplacement périphérique, CloudFront commence à transférer les demandes vers la nouvelle origine.

La modification de l'origine ne nécessite pas CloudFront de repeupler les caches périphériques avec des objets provenant de la nouvelle origine. Aussi longtemps que les demandes de l'utilisateur de votre application n'ont pas changé, CloudFront continue à servir les objets qui sont déjà dans un cache périphérique tant que la durée de vie (TTL) de chaque objet n'a pas expiré ou que les objets rarement demandés n'ont pas été évincés.

Protocole (origines personnalisées uniquement)

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

La politique de protocole que vous CloudFront souhaitez utiliser lors de la récupération d'objets depuis votre origine.

Choisissez l'une des valeurs suivantes :

- HTTP uniquement : CloudFront utilise uniquement le protocole HTTP pour accéder à l'origine.

  > **Important**
  >
  > HTTP only (HTTP uniquement) est le paramètre par défaut lorsque l'origine est un point de terminaison d'hébergement de site web statique Amazon S3, car Amazon S3 ne prend pas en charge les connexions HTTPS pour les points de terminaison d'hébergement de

sites web statiques. La CloudFront console ne prend pas en charge la modification de ce paramètre pour les points de terminaison d'hébergement de sites Web statiques Amazon S3.

- HTTPS uniquement : CloudFront utilise uniquement le protocole HTTPS pour accéder à l'origine.
- Match Viewer : CloudFront communique avec votre source via HTTP ou HTTPS, selon le protocole de la demande du spectateur. CloudFront ne met en cache l'objet qu'une seule fois, même si les utilisateurs font des demandes à l'aide des protocoles HTTP et HTTPS.

> **Important**
>
> Pour les demandes du lecteur HTTPS qui CloudFront sont transférées vers cette origine, l'un des noms de domaine figurant dans le SSL/TLS certificat de votre serveur d'origine doit correspondre au nom de domaine que vous avez spécifié pour le domaine d'origine. Sinon, CloudFront répond aux demandes du spectateur avec un code d'état HTTP 502 (Bad Gateway) au lieu de renvoyer l'objet demandé. Pour plus d’informations, consultez the section called “Exigences relatives à l'utilisation de SSL/TLS certificats avec CloudFront”.

Rubriques

- Port HTTP
- Port HTTPS
- Minimum de protocole SSL d’origine

Port HTTP

> **Note**
>
> Ceci s’applique uniquement aux origines personnalisées.

(Facultatif) Vous pouvez spécifier le port HTTP sur lequel l’origine personnalisée est à l’écoute. Valeurs valides : ports 80, 443, et 1024 à 65535. La valeur par défaut est le port 80.

> **Important**
>
> Le port 80 est le paramètre par défaut lorsque l'origine est un point de terminaison d'hébergement de site web statique Amazon S3, car Amazon S3 prend uniquement en charge le port 80 pour les points de terminaison d'hébergement de sites web statiques. La CloudFront console ne prend pas en charge la modification de ce paramètre pour les points de terminaison d'hébergement de sites Web statiques Amazon S3.

Port HTTPS

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

(Facultatif) Vous pouvez spécifier le port HTTPS sur lequel l'origine personnalisée est à l'écoute. Valeurs valides : ports 80, 443, et 1024 à 65535. La valeur par défaut est le port 443. Quand Protocol (Protocole) a la valeur HTTP only (HTTP uniquement), vous ne pouvez pas spécifier une valeur pourHTTPS port (Port HTTPS).

Minimum de protocole SSL d'origine

> **Note**
>
> Ceci s'applique uniquement aux origines personnalisées.

Choisissez le TLS/SSL protocole minimal à CloudFront utiliser lorsqu'il établit une connexion HTTPS avec votre point d'origine. Les protocoles TLS inférieurs sont moins sécurisés, nous vous recommandons donc de choisir le dernier protocole TLS que votre origine prend en charge. QuandProtocol (Protocole) a la valeur HTTP only (HTTP uniquement), vous ne pouvez pas spécifier une valeur pour Minimum origin SSL protocol (Minimum de protocole SSL d'origine).

Si vous utilisez l' CloudFront API pour définir le TLS/SSL protocole CloudFront à utiliser, vous ne pouvez pas définir de protocole minimum. Au lieu de cela, vous spécifiez tous les TLS/SSL protocoles qui CloudFront peuvent être utilisés avec votre origine. Pour plus d'informations, consultez OriginSslProtocolsle Amazon CloudFront API Reference.

Chemin d’origine

Si vous souhaitez demander votre contenu CloudFront à partir d'un répertoire de votre origine, entrez le chemin du répertoire, en commençant par une barre oblique (/). CloudFront ajoute le chemin du répertoire à la valeur du domaine d'origine, par exemple,**`cf-origin.example.com/production/images`**. N’ajoutez pas un slash (/) à la fin du chemin d’accès.

Imaginons que vous ayez, par exemple, les valeurs suivantes pour votre distribution :

- Domaine d’origine : compartiment Amazon S3 nommé **`amzn-s3-demo-bucket`**
- Chemin d’origine : **`/production`**
- Noms de domaine alternatifs (CNAME) : **`example.com`**

Lorsqu'un utilisateur entre `example.com/index.html` dans un navigateur, il CloudFront envoie une demande à Amazon S3 pour`amzn-s3-demo-bucket/production/index.html`.

Lorsqu'un utilisateur entre `example.com/acme/index.html` dans un navigateur, il CloudFront envoie une demande à Amazon S3 pour`amzn-s3-demo-bucket/production/acme/index.html`.

Nom

Un nom est une chaîne qui identifie de façon unique cette origine dans cette distribution. Vous pouvez créer des comportements de cache en plus du comportement de cache par défaut. Dans ce cas, vous utilisez le nom que vous spécifiez ici pour identifier l'origine CloudFront vers laquelle vous souhaitez acheminer une demande lorsque la demande correspond au modèle de chemin correspondant à ce comportement de cache.

Accès à l'origine (origines Amazon S3 uniquement)

> **Note**
>
> Cela s’applique uniquement aux origines du compartiment Amazon S3 (celles qui n’utilisent pas le point de terminaison statique du site web S3).

Choisissez les paramètres de contrôle d'accès Origin (recommandés) si vous souhaitez permettre de restreindre l'accès à l'origine d'un compartiment Amazon S3 à des CloudFront distributions spécifiques uniquement.

Choisissez Public si l'origine du compartiment Amazon S3 est accessible au public.

Pour plus d'informations, consultez the section called “Restriction de l'accès à une origine Amazon S3”.

Pour plus d'informations sur la manière d'obliger les utilisateurs à accéder à des objets sur une origine personnalisée en utilisant uniquement CloudFront des URL, consultezthe section called “Restriction de l'accès à des fichiers d'origines personnalisées”.

Ajout d'en-tête personnalisé

Si vous CloudFront souhaitez ajouter des en-têtes personnalisés chaque fois qu'une demande est envoyée à votre origine, spécifiez le nom de l'en-tête et sa valeur. Pour plus d'informations, consultez the section called “Ajout d'en-têtes personnalisés aux demandes d'origine”.

Pour obtenir le nombre maximum actuel d'en-têtes personnalisés que vous pouvez ajouter, la longueur maximale d'un nom et d'une valeur d'en-tête personnalisé, et la longueur totale maximale de tous les noms et valeurs d'en-tête, consultez Quotas.

Activer Origin Shield

Choisissez Oui pour activer CloudFront Origin Shield. Pour plus d'informations au sujet de Origin Shield, consultez the section called “Utilisation d'Origin Shield”.

Tentatives de connexion

Vous pouvez définir le nombre de CloudFront tentatives de connexion à l'origine. Vous pouvez spécifier 1, 2 ou 3 tentatives. Le nombre par défaut (sauf indication contraire) est 3.

Utilisez ce paramètre avec le délai d'expiration de la connexion pour spécifier le temps d' CloudFront attente avant de tenter de vous connecter à l'origine secondaire ou de renvoyer une réponse d'erreur au visualiseur. Par défaut, CloudFront attend jusqu'à 30 secondes (3 tentatives de 10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d'attente de connexion plus court, ou les deux.

Si le nombre de tentatives de connexion spécifié échoue, CloudFront effectue l'une des opérations suivantes :

- Si l'origine fait partie d'un groupe d'origine, CloudFront tente de se connecter à l'origine secondaire. Si le nombre spécifié de tentatives de connexion à l'origine secondaire échouent, CloudFront renvoie une réponse d'erreur au visualiseur.
- Si l'origine ne fait pas partie d'un groupe d'origine, CloudFront renvoie une réponse d'erreur au visualiseur.

Pour une origine personnalisée (y compris un compartiment Amazon S3 configuré avec un hébergement de site Web statique), ce paramètre spécifie également le nombre de CloudFront tentatives d'obtention d'une réponse de la part de l'origine. Pour plus d'informations, consultez the section called “Délai de réponse”.

Délai de connexion

Le délai d'expiration de la connexion est le nombre de secondes qui CloudFront attendent lorsque vous essayez d'établir une connexion avec l'origine. Vous pouvez spécifier un nombre de secondes compris entre 1 et 10 (inclus). Le délai d'expiration par défaut (sauf indication contraire) est de 10 secondes.

Utilisez ce paramètre avec les tentatives de connexion pour spécifier le temps d' CloudFront attente avant de tenter de vous connecter à l'origine secondaire ou avant de renvoyer une réponse d'erreur au visualiseur. Par défaut, CloudFront attend jusqu'à 30 secondes (3 tentatives de 10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d'attente de connexion plus court, ou les deux.

S'il CloudFront n'établit pas de connexion avec l'origine dans le délai de secondes spécifié, CloudFront effectue l'une des opérations suivantes :

- Si le nombre de tentatives de connexion spécifié est supérieur à 1, CloudFront essaie à nouveau d'établir une connexion. CloudFront essaie jusqu'à 3 fois, en fonction de la valeur des tentatives de connexion.
- Si toutes les tentatives de connexion échouent et que l'origine fait partie d'un groupe d'origine, CloudFront tente de se connecter à l'origine secondaire. Si le nombre spécifié de tentatives de connexion à l'origine secondaire échouent, CloudFront renvoie une réponse d'erreur au visualiseur.
- Si toutes les tentatives de connexion échouent et que l'origine ne fait pas partie d'un groupe d'origine, CloudFront renvoie une réponse d'erreur au visualiseur.

Délai de réponse

Le délai de réponse de l'origine, également appelé délai de demande à l'origine ou délai d'attente des opérations de lecture depuis l'origine, s'applique aux deux valeurs suivantes :

- Durée (en secondes) d' CloudFront attente d'une réponse après avoir transmis une demande à l'origine.
- Durée (en secondes) d' CloudFront attente après réception d'un paquet de réponse de l'origine et avant de recevoir le paquet suivant.

> **Tip**
>
> Si vous souhaitez augmenter la valeur de délai de réponse de l'origine parce que les utilisateurs rencontrent des erreurs de code d'état HTTP 504, envisagez d'explorer d'autres moyens pour éliminer ces erreurs avant de modifier la valeur de délai. Consultez les suggestions de dépannage dans the section called "Code d'état HTTP 504 (Délai d'attente de passerelle expiré)".

CloudFront le comportement dépend de la méthode HTTP utilisée dans la requête du visualiseur :

- `GET`et `HEAD` demandes : si l'origine ne répond pas ou cesse de répondre dans le délai imparti, interrompt CloudFront la connexion. CloudFront essaie à nouveau de se connecter en fonction de la valeur dethe section called "Tentatives de connexion".
- `DELETE`,`OPTIONS`, `PATCH`PUT, et `POST` demandes : si l'origine ne répond pas pendant le délai de lecture, interrompt CloudFront la connexion et n'essaie plus de contacter l'origine. Le client peut soumettre à nouveau la demande si nécessaire.

Délai d'exécution de la réponse

> **Note**
>
> Le délai d'exécution de la réponse ne prend pas en charge la fonctionnalité de déploiement continu.

Durée (en secondes) pendant laquelle une demande provenant CloudFront de l'origine peut rester ouverte et attendre une réponse. Si la réponse complète n'est pas reçue de l'origine à ce moment-là, CloudFront met fin à la connexion.

Contrairement au délai de réponse, qui est le temps d'attente pour les paquets de réponse individuels, le délai d'expiration de la réponse est le temps d'CloudFront attente maximal autorisé pour la fin de la réponse. Vous pouvez utiliser ce paramètre pour vous assurer qu'une origine lente ou CloudFront ne répond pas indéfiniment, même si d'autres paramètres de délai d'attente autorisent une attente plus longue.

Ce délai d'attente maximal inclut ce que vous avez défini pour les autres paramètres de délai d'attente ainsi que le nombre de Tentatives de connexion effectuées pour chaque nouvelle tentative. Vous pouvez utiliser ces paramètres ensemble pour spécifier le temps d' CloudFront attente pour la demande complète et le moment où il faut y mettre fin, qu'elle soit complète ou non.

Par exemple, si vous définissez les paramètres suivants :

- Tentatives de connexion définies sur 3
- Délai de connexion défini sur 10 secondes
- Délai de réponse défini sur 30 secondes
- Délai d'exécution de la réponse défini sur 60 secondes

Cela signifie qu' CloudFront il essaiera de se connecter à l'origine (jusqu'à 3 tentatives au total), chaque tentative de connexion expirant au bout de 10 secondes. Une fois connectée, l'origine CloudFront attendra jusqu'à 30 secondes pour que l'origine réponde à la demande jusqu'à ce qu'elle reçoive le dernier paquet de la réponse.

Quel que soit le nombre de tentatives de connexion ou le délai de réponse, la connexion CloudFront sera interrompue si la réponse complète de l'origine prend plus de 60 secondes. CloudFront renverra ensuite au visualiseur une réponse the section called "Code d'état HTTP 504 (Délai d'attente de passerelle expiré)" d'erreur ou une réponse d'erreur personnalisée si vous en avez spécifié une.

> **Remarques**
>
> - Si vous définissez une valeur pour le délai d'exécution de la réponse, celle-ci doit être égale ou supérieure à la valeur du Délai de réponse (délai de lecture d'origine).

- Si vous ne définissez pas de valeur pour le délai d'expiration de la réponse, CloudFront cela n'impose pas de valeur maximale.

Keep-alive délai d'expiration (origines personnalisées et VPC uniquement)

Le délai de conservation correspond à la durée (en secondes) des CloudFront tentatives de maintien d'une connexion à votre origine personnalisée après réception du dernier paquet de réponse. Maintenir une connexion persistante permet de gagner le temps requis pour ré-établir la connexion TCP et établir une autre liaison TLS pour les demandes ultérieures. Augmenter le délai d'inactivité contribue à améliorer la métrique de demande par connexion pour les distributions.

> **Note**
>
> Pour que la valeur du Keep-alive délai d'expiration ait un effet, votre origine doit être configurée pour autoriser les connexions persistantes.

Quotas de délai de réponse et d'attente des connexions actives

- La valeur par défaut pour le Délai de réponse est de 30 secondes.
- La valeur par défaut du Délai d'attente des connexions actives est de 5 secondes.

Si vous demandez une augmentation du délai d'expiration pour votre distribution Compte AWS, mettez à jour les origines de votre distribution afin qu'elles présentent les valeurs de délai de réponse et de délai de maintien en vie que vous souhaitez. Une augmentation de quota pour votre compte ne met pas automatiquement à jour vos origines. Par exemple, si vous utilisez une fonction Lambda@Edge pour définir un délai d'attente des connexions actives de 90 secondes, l'origine doit déjà être configurée avec un délai d'attente des connexions actives d'au moins 90 secondes. Dans le cas contraire, votre fonction Lambda@Edge risque de ne pas s'exécuter.

Pour en savoir plus sur les quotas des distributions, y compris la procédure pour demander une augmentation, consultez Quotas généraux sur les distributions.

Paramètres de comportement du cache

En définissant le comportement du cache, vous pouvez configurer diverses CloudFront fonctionnalités pour un modèle de chemin d'URL donné pour les fichiers de votre site Web. Par

exemple, un comportement de cache peut s'appliquer à tous les fichiers `.jpg` du répertoire `images` d'un serveur web que vous utilisez comme serveur d'origine pour CloudFront. Les fonctionnalités que vous pouvez configurer pour chaque comportement de cache sont les suivantes :

- Le modèle de chemin d’accès
- Si vous avez configuré plusieurs origines pour votre CloudFront distribution, l'origine vers laquelle vous CloudFront souhaitez transférer vos demandes
- S’il convient ou non de transférer les chaînes de requête à votre origine
- Si l’accès aux fichiers spécifiés requiert ou non des URL signées
- S’il convient ou non d’exiger que les utilisateurs utilisent HTTPS pour accéder à ces fichiers
- Durée minimale pendant laquelle ces fichiers restent dans le CloudFront cache, quelle que soit la valeur des `Cache-Control` en-têtes ajoutés aux fichiers par votre origine

Lorsque vous créez une distribution, vous spécifiez les paramètres du comportement de cache par défaut, lequel achemine automatiquement toutes les demandes vers l’origine que vous spécifiez lors de la création de la distribution. Après avoir créé une distribution, vous pouvez créer des comportements de cache supplémentaires qui définissent le mode de CloudFront réponse lorsqu'il reçoit une demande d'objets correspondant à un modèle de chemin, par exemple,`*.jpg`. Si vous créez des comportements de cache supplémentaires, le comportement de cache par défaut est toujours le dernier à être traité. Les autres comportements de cache sont traités dans l'ordre dans lequel ils sont répertoriés dans la CloudFront console ou, si vous utilisez l' CloudFront API, dans l'ordre dans lequel ils sont répertoriés dans l'`DistributionConfig`élément de distribution. Pour plus d’informations, consultez Modèle de chemin.

Lorsque vous créez un comportement de cache, vous spécifiez l'origine à partir de laquelle vous CloudFront souhaitez obtenir les objets. Par conséquent, si vous CloudFront souhaitez distribuer des objets provenant de toutes vos origines, vous devez avoir au moins autant de comportements de cache (y compris le comportement de cache par défaut) que d'origines. Par exemple, si vous avez deux origines et que vous utilisez uniquement le comportement de cache par défaut, le comportement de cache par défaut permet d'obtenir des objets CloudFront à partir de l'une des origines, mais l'autre origine n'est jamais utilisée.

Pour connaître le nombre maximum actuel de comportements de cache que vous pouvez ajouter à une distribution ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas généraux sur les distributions.

Rubriques

- Modèle de chemin
- Origine ou groupe d’origines
- Viewer Protocol Policy
- Méthodes HTTP autorisées
- Field-level configuration de chiffrement
- Méthodes HTTP mises en cache
- Autoriser les requêtes gRPC sur HTTP/2
- Mise en cache basée sur des en-têtes de demande sélectionnés
- En-têtes de la liste d’autorisation
- Mise en cache d’un objet
- Durée de vie minimale
- Durée de vie (TTL) maximale
- TTL par défaut
- Réacheminer les cookies
- Cookies de la liste d’autorisation
- Réacheminement et mise en cache des chaînes de requête
- Liste d’autorisation des chaînes de requête
- Smooth Streaming
- Restreindre l’accès des utilisateurs (utiliser des URL signées ou des cookies signés)
- Signataires autorisés
- Compte AWS nombres
- Compresser des objets automatiquement
- CloudFront événement
- ARN de fonction Lambda
- Inclure le corps

Modèle de chemin

Un modèle de chemin d’accès (par exemple, `images/*.jpg`) spécifie les demandes auxquelles vous voulez que ce comportement de cache s’applique. Lors de la CloudFront réception d'une demande d'utilisateur final, le chemin demandé est comparé aux modèles de chemin dans

l'ordre dans lequel les comportements du cache sont répertoriés dans la distribution. La première correspondance détermine le comportement de cache qui s'applique à la demande. Imaginons, par exemple, que vous ayez trois comportements de cache avec les trois modèles de chemin suivants classés par ordre :

- `images/*.jpg`
- `images/*`
- `*.gif`

> **Note**
>
> Vous pouvez éventuellement inclure une barre oblique (/) au début du modèle de tracé, par exemple,`/images/*.jpg`. CloudFront le comportement est le même avec ou sans le premier /. Si vous ne spécifiez pas le/au début du chemin, ce caractère est automatiquement implicite ; CloudFront traite le chemin de la même manière, avec ou sans le premier /. Par exemple, CloudFront traite `/*product.jpg` la même chose que `*product.jpg`

Une demande du fichier `images/sample.gif` ne correspondant pas au premier modèle de chemin d'accès, les comportements de cache associés ne s'appliquent pas à la demande. Comme le fichier satisfait bel et bien au second modèle, les comportements de cache associés au deuxième modèle s'appliquent même si la demande correspond aussi au troisième modèle.

> **Note**
>
> Lorsque vous créez une distribution, la valeur de Modèle de chemin pour le comportement de cache par défaut est définie sur * (tous les fichiers) et ne peut pas être modifiée. Cette valeur CloudFront entraîne le transfert de toutes les demandes relatives à vos objets vers l'origine que vous avez spécifiée dans le Domaine d'origine champ. Si la demande d'un objet ne correspond au modèle de chemin d'aucun autre comportement de cache, CloudFront applique le comportement que vous spécifiez dans le comportement de cache par défaut.

> **Important**
>
> Définissez soigneusement les modèles de chemin et leur séquence, sans quoi vous risquez d'offrir aux utilisateurs un accès non souhaité à votre contenu. Par exemple,

imaginons qu'une demande corresponde au modèle de chemin de deux comportements de cache. Le premier comportement de cache n'exige pas d'URL signées, à l'inverse du second comportement de cache. Les utilisateurs peuvent accéder aux objets sans utiliser d'URL signée car CloudFront traite le comportement du cache associé à la première correspondance.

Si vous travaillez avec un MediaPackage canal, vous devez inclure des modèles de chemin spécifiques pour le comportement du cache que vous définissez pour le type de point de terminaison de votre origine. Par exemple, pour un point de terminaison DASH, tapez `*.mpd` pour Path Pattern (Modèle de chemin). Pour plus d'informations et pour obtenir des instructions spécifiques, consultez Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage.

Le chemin que vous spécifiez s'applique aux demandes pour tous les fichiers du répertoire spécifié et des sous-répertoires situés sous le répertoire spécifié. CloudFront ne prend pas en compte les chaînes de requête ou les cookies lors de l'évaluation du modèle de chemin. Par exemple, si un répertoire `images` contient les sous-répertoires `product1` et `product2`, le modèle de chemin d'accès `images/*.jpg` s'applique aux demandes concernant un fichier .jpg des répertoires `images`, `images/product1` et `images/product2`. Si vous voulez appliquer un autre comportement de cache aux fichiers du répertoire `images/product1` qu'à ceux des répertoires `images` et `images/product2`, créez un comportement de cache distinct pour `images/product1` et déplacez ce comportement de cache vers un emplacement au-dessus (avant) du comportement de cache du répertoire `images`.

Vous pouvez utiliser les caractères génériques suivants dans votre modèle de chemin d'accès :

- `*` correspond à 0 caractère ou plus.
- `?` correspond à 1 caractère exactement.

L'exemple suivant montre le fonctionnement des caractères génériques :

Modèle de chemin d'accès	Fichiers correspondant au modèle de chemin d'accès
`*.jpg`	Tous les fichiers .jpg.

Modèle de chemin d'accès	Fichiers correspondant au modèle de chemin d'accès
`images/*.jpg`	Tous les fichiers .jpg dans le répertoire `images` et dans les sous-répertoires du répertoire `images`.
`a*.jpg`	• Tous les fichiers .jpg dont le nom commence par `a` : par exemple, `apple.jpg` et `appalachian_trail_2012_05_21.jpg` . • Tous les fichiers .jpg dont le chemin d'accès commence par `a` : par exemple, `abra/cadabra/magic.jpg` .
`a??.jpg`	Tous les fichiers .jpg dont le nom commence par `a`, suivi de deux autres caractères exactement : par exemple, `ant.jpg` et `abe.jpg`.
`*.doc*`	Tous les fichiers .jpg dont l'extension de nom de fichier commence par `.doc` : par exemple, les fichiers `.doc`, `.docx` et `.docm`. Vous ne pouvez pas utiliser le modèle de chemin d'accès `*.doc?` dans ce cas, parce que ce modèle ne s'appliquerait pas aux demandes relatives aux fichiers `.doc` ; le caractère générique `?` remplace exactement un seul caractère.

La longueur maximale d'un modèle de chemin est de 255 caractères. La valeur peut contenir l'un des caractères suivants :

- A-Z, a-z

  Les modèles de chemin d'accès étant sensibles à la casse, le modèle de chemin d'accès `*.jpg` ne s'applique pas au fichier `LOGO.JPG`.
- 0-9
- _ - . * $ / ~ " ' @ : +
- &, transmis et renvoyé comme `&`

Normalisation du chemin

CloudFront normalise les chemins d'URI conformément à la RFC 3986, puis fait correspondre le chemin avec le comportement de cache correct. Une fois que le comportement du cache correspond, CloudFront envoie le chemin d'URI brut à l'origine. Si aucune correspondance n'est trouvée, les demandes sont plutôt dirigées vers votre comportement de cache par défaut.

Certains caractères sont normalisés et supprimés du chemin, tels que les barres obliques multiples (`//`) ou les points successifs (`..`). Cela peut modifier l'URL CloudFront utilisée pour qu'elle corresponde au comportement de cache prévu.

Example Exemple

Vous spécifiez les chemins `/a/b*` et `/a*` pour le comportement de votre cache.

- Lorsqu'un utilisateur envoie le chemin `/a/b?c=1`, CloudFront le fera correspondre au comportement de cache `/a/b*`.
- Lorsqu'un utilisateur envoie le chemin `/a/b/..?c=1`, CloudFront le fera correspondre au comportement de cache `/a*`.

Pour contourner la normalisation des chemins, vous pouvez mettre à jour les chemins de vos demandes ou le modèle de chemin utilisé par le comportement de cache.

Origine ou groupe d'origines

Ce paramètre s'applique uniquement lorsque vous créez ou mettez à jour un comportement de cache pour une distribution existante.

Entrez la valeur d'une origine ou d'un groupe d'origines existant. Cela identifie l'origine ou le groupe d'origine vers lequel vous souhaitez CloudFront acheminer les demandes lorsqu'une demande (telle quehttps://example.com/logo.jpg) correspond au modèle de chemin d'un comportement de cache (tel que *.jpg) ou au comportement de cache par défaut (*).

Viewer Protocol Policy

Choisissez la politique de protocole que vous souhaitez que les spectateurs utilisent pour accéder à votre contenu dans des emplacements CloudFront périphériques :

- HTTP et HTTPS : les deux protocoles peuvent être utilisés.

- Rediriger HTTP vers HTTPS : les deux protocoles peuvent être utilisés, mais les requêtes HTTP sont automatiquement redirigées vers des requêtes HTTPS.
- HTTPS uniquement : l'accès au contenu ne peut se faire qu'à l'aide du protocole HTTPS.

Pour plus d'informations, consultez Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.

Méthodes HTTP autorisées

Spécifiez les méthodes HTTP que vous CloudFront souhaitez traiter et transmettre à votre origine :

- GET, HEAD : Vous ne pouvez l'utiliser CloudFront que pour récupérer des objets depuis votre origine ou pour obtenir des en-têtes d'objets.
- GET, HEAD, OPTIONS : Vous pouvez utiliser CloudFront uniquement pour obtenir les objets de votre origine, récupérer les en-têtes d'objet ou extraire la liste des options que votre serveur d'origine prend en charge.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE : vous pouvez les utiliser CloudFront pour obtenir, ajouter, mettre à jour et supprimer des objets, ainsi que pour obtenir des en-têtes d'objets. De plus, vous pouvez exécuter d'autres opérations POST telles que l'envoi de données à partir d'un formulaire web.

> **Note**
>
> Si vous utilisez le framework gRPC dans votre charge de travail, vous devez sélectionner GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. Les charges de travail gRPC nécessitent la méthode `POST`. Pour plus d'informations, consultez Utilisation de gRPC avec des distributions CloudFront.
> CloudFront met en cache les réponses aux `HEAD` demandes `GET` et, éventuellement, `OPTIONS` aux demandes. Les réponses aux `OPTIONS` demandes sont mises en cache séparément des réponses aux `HEAD` demandes `GET` et aux demandes (la `OPTIONS` méthode est incluse dans la clé de cache pour les `OPTIONS` demandes). CloudFront ne met pas en cache les réponses aux demandes utilisant d'autres méthodes.

Important

Si vous choisissez GET, HEAD, OPTIONS ou GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE, il se peut que vous ayez besoin de limiter l'accès à votre compartiment Amazon S3 ou à votre origine personnalisée pour empêcher que les utilisateurs n'exécutent des opérations qu'ils ne sont pas autorisés à faire. Les exemples suivants expliquent comment limiter l'accès :

- Si vous utilisez Amazon S3 comme origine pour votre distribution : créez un contrôle CloudFront d'accès à l'origine pour restreindre l'accès à votre contenu Amazon S3 et autorisez le contrôle d'accès à l'origine. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes uniquement parce que vous souhaitez les utiliserPUT, vous devez tout de même configurer les politiques de compartiment Amazon S3 afin de traiter les `DELETE` demandes de manière appropriée. Pour plus d'informations, consultez Restriction de l'accès à une origine Amazon S3.
- Si vous utilisez une origine personnalisée : configurez votre serveur d'origine pour qu'il gère toutes les méthodes. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes uniquement parce que vous souhaitez les utiliser`POST`, vous devez tout de même configurer votre serveur d'origine pour traiter les `DELETE` demandes de manière appropriée.

Field-level configuration de chiffrement

Si vous souhaitez appliquer un chiffrement au niveau du champ à des champs de données spécifiques, dans la liste déroulante, choisissez une configuration de chiffrement au niveau du champ.

Pour plus d'informations, consultez Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.

Méthodes HTTP mises en cache

Spécifiez si vous souhaitez CloudFront mettre en cache la réponse depuis votre origine lorsqu'un utilisateur envoie une `OPTIONS` demande. CloudFront met toujours en cache les réponses `GET` et les `HEAD` demandes.

Autoriser les requêtes gRPC sur HTTP/2

Indiquez si vous souhaitez que votre distribution autorise les demandes gRPC. Pour activer gRPC, sélectionnez les paramètres suivants :

- Pour les Méthodes HTTP autorisées, sélectionnez les méthode GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. gRPC nécessite la méthode `POST`.
- Cochez la case gRPC qui apparaît après avoir sélectionné la méthode `POST`.
- Pour Versions de HTTP prises en charge, sélectionnez HTTP/2.

Pour plus d'informations, consultez Utilisation de gRPC avec des distributions CloudFront.

Mise en cache basée sur des en-têtes de demande sélectionnés

Spécifiez si vous souhaitez CloudFront mettre en cache les objets en fonction des valeurs des en-têtes spécifiés :

- Aucune (améliore la mise en cache) : CloudFront ne met pas en cache vos objets en fonction des valeurs d'en-tête.
- Allowlist — met en CloudFront cache vos objets en fonction uniquement des valeurs des en-têtes spécifiés. Utilisez Allowlist Headers pour choisir les en-têtes sur lesquels vous souhaitez CloudFront baser la mise en cache.
- Tout : CloudFront ne met pas en cache les objets associés à ce comportement de cache. Au lieu de cela, CloudFront envoie chaque demande à l'origine. (Déconseillé pour les origines Amazon S3.)

Quelle que soit l'option que vous choisissez, CloudFront redirige certains en-têtes vers votre origine et prend des mesures spécifiques en fonction des en-têtes que vous transférez. Pour plus d'informations sur le mode de CloudFront gestion du transfert d'en-têtes, consultezEn-têtes et CloudFront comportement des requêtes HTTP (origines personnalisées et Amazon S3).

Pour plus d'informations sur la configuration de la mise en cache à l'aide CloudFront des en-têtes de demande, consultez. Mise en cache de contenu basée sur des en-têtes de demandes

En-têtes de la liste d'autorisation

Ces paramètres s'appliquent uniquement lorsque vous choisissez Allowlist pour Mise en cache basée sur des en-têtes de demande sélectionnés.

Spécifiez les en-têtes que vous souhaitez prendre en compte lors CloudFront de la mise en cache de vos objets. Sélectionnez les en-têtes dans la liste des en-têtes disponibles et choisissez Ajouter. Pour transmettre un en-tête personnalisé, entrez le nom de l'en-tête dans le champ et choisissez Ajouter un en-tête personnalisé.

Pour connaître le nombre maximal actuel d'en-têtes qu'il est possible d'ajouter en liste d'autorisation pour chaque comportement de cache, ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas sur les en-têtes.

Mise en cache d'un objet

Si votre serveur d'origine ajoute un `Cache-Control` en-tête à vos objets pour contrôler la durée pendant laquelle les objets restent dans le CloudFront cache et si vous ne souhaitez pas modifier la `Cache-Control` valeur, choisissez Utiliser les en-têtes du cache d'origine.

Pour définir la durée minimale et maximale pendant laquelle vos objets restent dans le CloudFront cache, quels que soient `Cache-Control` les en-têtes, et la durée par défaut pendant laquelle vos objets restent dans le CloudFront cache lorsque l'`Cache-Control`en-tête est absent d'un objet, choisissez Personnaliser. Puis, dans les champs Durée de vie minimale, Durée de vie par défaut et Durée de vie maximale, spécifiez la valeur applicable.

Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Durée de vie minimale

Spécifiez la durée minimale, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant d' CloudFront envoyer une autre demande à l'origine pour déterminer si l'objet a été mis à jour.

> **Warning**
>
> Si votre TTL minimum est supérieur à 0, le contenu CloudFront sera mis en cache pendant au moins la durée spécifiée dans le TTL minimum de la politique de cache, même si les `private` directives `Cache-Control: no-cache` `no-store`, ou sont présentes dans les en-têtes d'origine.

Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Durée de vie (TTL) maximale

Spécifiez la durée maximale, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de demander CloudFront à votre origine si l'objet a été mis à jour. La valeur que vous spécifiez pour Durée de vie maximale s'applique uniquement quand votre origine ajoute aux objets les en-têtes HTTP tels que `Cache-Control max-age`, `Cache-Control s-maxage` ou `Expires`. Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Pour spécifier une valeur pour Durée de vie maximale, vous devez choisir l'option Personnaliser pour le paramètre Mise en cache d'un objet.

La valeur par défaut de Durée de vie maximale est 31 536 000 secondes (soit 1 année). Si vous remplacez la valeur de Durée de vie minimale ou Durée de vie par défaut par une valeur supérieure à 31 536 000 secondes, la valeur par défaut de Durée de vie maximale prend la valeur de Durée de vie par défaut.

TTL par défaut

Spécifiez la durée par défaut, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de transmettre une CloudFront autre demande à votre origine afin de déterminer si l'objet a été mis à jour. La valeur que vous spécifiez pour TTL par défaut s'applique uniquement quand votre origine n'ajoute pas des en-têtes HTTP tels que `Cache-Control max-age`, `Cache-Control s-maxage` ou `Expires` aux objets. Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Pour spécifier une valeur pour Durée de vie par défaut, vous devez choisir l'option Personnaliser pour le paramètre Mise en cache d'un objet.

La valeur par défaut de Durée de vie par défaut est 86 400 secondes (soit 1 journée). Si vous remplacez la valeur de Durée de vie minimale par une valeur supérieure à 86 400 secondes, la valeur par défaut de Durée de vie par défaut prend la valeur de Durée de vie minimale.

Réacheminer les cookies

> **Note**
>
> Pour les origines Amazon S3, cette option s'applique uniquement aux compartiments configurés en tant que point de terminaison de site Web.

Spécifiez si vous CloudFront souhaitez transférer les cookies vers votre serveur d'origine et, dans l'affirmative, lesquels. Si vous choisissez de transférer uniquement les cookies sélectionnés (liste d’autorisation de cookies), entrez les noms de cookies dans le champ Cookies de la liste d’autorisation. Si vous choisissez Tous, CloudFront transmet tous les cookies, quel que soit le nombre utilisé par votre application.

Amazon S3 ne traite pas les cookies, et la transmission des cookies à l’origine réduit la capacité de mise en cache. Pour les comportements de cache qui transmettent les demandes à une origine Amazon S3, choisissez None (Aucun) pour Forward Cookies (Réacheminer les cookies).

Pour plus d’informations sur la transmission des cookies à l’origine, consultez Mise en cache de contenu basée sur des cookies.

Cookies de la liste d’autorisation

> **Note**
>
> Pour les origines Amazon S3, cette option s’applique uniquement aux compartiments configurés en tant que point de terminaison de site Web.

Si vous avez choisi Allowlist dans la liste des cookies de transfert, entrez dans le champ Allowlist Cookies les noms des cookies que vous souhaitez transférer CloudFront vers votre serveur d'origine pour ce comportement de cache. Entrez chaque nom de cookie sur une nouvelle ligne.

Vous pouvez utiliser les caractères génériques suivants pour spécifier les noms de cookie :

- * correspond à 0 caractère ou plus dans le nom de cookie
- ? correspond à 1 caractère exactement dans le nom de cookie.

Imaginons, par exemple, qu’une demande inclue un cookie nommé :

`userid_`*`member-number`*

Où chacun de vos utilisateurs possède une valeur unique pour*`member-number`*. Vous souhaitez CloudFront mettre en cache une version distincte de l'objet pour chaque membre. Vous pouvez y parvenir en transférant tous les cookies vers votre source, mais les demandes des utilisateurs incluent certains cookies que vous ne souhaitez pas mettre CloudFront en cache. Vous pouvez

également spécifier la valeur suivante comme nom de cookie, ce qui entraîne CloudFront le transfert à l'origine de tous les cookies commençant par `userid_` :

```
userid_*
```

Pour connaître le nombre maximal actuel de noms de cookies qu'il est possible d'ajouter en liste d'autorisation pour chaque comportement de cache, ou pour demander un quota plus élevé (auparavant appelé limite), consultez Quotas sur les cookies (paramètres de cache hérités).

Réacheminement et mise en cache des chaînes de requête

CloudFront peut mettre en cache différentes versions de votre contenu en fonction des valeurs des paramètres de chaîne de requête. Choisissez l'une des options suivantes :

Aucun (optimise la mise en cache)

> Choisissez cette option si votre origine renvoie la même version d'un objet quelles que soient les valeurs des paramètres de la chaîne de requête. Cela augmente la probabilité de CloudFront répondre à une demande depuis le cache, ce qui améliore les performances et réduit la charge sur votre origine.

Tout réacheminer, cache basé sur la liste d'autorisation

> Sélectionnez cette option si votre serveur d'origine renvoie des versions différentes de vos objets en fonction d'un ou de plusieurs paramètres de la chaîne de requête. Spécifiez ensuite les paramètres que vous CloudFront souhaitez utiliser comme base pour la mise en cache dans le Liste d'autorisation des chaînes de requête champ.

Tout réacheminer, cache basé sur tout

> Sélectionnez cette option si votre serveur d'origine renvoie des versions différentes de vos objets en fonction de tous les paramètres de la chaîne de requête.

Pour plus d'informations sur la mise en cache en fonction des paramètres de la chaîne de requête, y compris sur la façon d'améliorer les performances, consultez la page Mise en cache de contenu basée sur les paramètres de chaîne de requête.

Liste d'autorisation des chaînes de requête

Ce paramètre s'applique uniquement lorsque vous choisissez Tout réacheminer, cache basé sur la liste d'autorisation pour Réacheminement et mise en cache des chaînes de requête. Vous pouvez

spécifier les paramètres de chaîne de requête que vous CloudFront souhaitez utiliser comme base pour la mise en cache.

Smooth Streaming

Choisissez Oui si vous voulez distribuer des fichiers multimédias au format Microsoft Smooth Streaming et que vous n'avez pas de serveur IIS.

Choisissez Non si vous avez un serveur Microsoft IIS que vous souhaitez utiliser comme origine pour distribuer des fichiers multimédias au format Microsoft Smooth Streaming ou si vous ne distribuez pas de fichiers multimédias Smooth Streaming.

> **Note**
>
> Si vous spécifiez Oui, vous pouvez continuer à distribuer d'autres contenus en utilisant ce comportement de cache s'ils correspondent à la valeur de Modèle de chemin.

Pour plus d'informations, consultez Configuration de vidéo à la demande pour Microsoft Smooth Streaming.

Restreindre l'accès des utilisateurs (utiliser des URL signées ou des cookies signés)

Si vous voulez des demandes d'objets qui correspondent à la valeur de `PathPattern` pour que le comportement de cache utilise des URL publiques, choisissez Non.

Si vous voulez des demandes d'objets qui correspondent à la valeur de `PathPattern` pour que le comportement de cache utilise des URL signées, choisissez Oui. Spécifiez ensuite les AWS comptes que vous souhaitez utiliser pour créer des URL signées ; ces comptes sont appelés signataires approuvés.

Pour plus d'informations sur les utilisateurs de confiance, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.

Signataires autorisés

Ce paramètre s'applique uniquement lorsque vous choisissez Oui pour Restreindre l'accès des utilisateurs (Utiliser des URL signées ou des Cookies signés).

Choisissez les AWS comptes que vous souhaitez utiliser comme signataires approuvés pour ce comportement de cache :

- Auto-signature : utilisez le compte avec lequel vous êtes actuellement connecté en Console de gestion AWS tant que signataire de confiance. Si vous êtes actuellement connecté en tant qu'utilisateur IAM, le AWS compte associé est ajouté en tant que signataire de confiance.
- Spécifier des comptes : saisissez les numéros de comptes des utilisateurs de confiance dans le champ Numéros de comptes AWS .

Pour créer des URL signées, un AWS compte doit disposer d'au moins une paire de CloudFront clés active.

> **Important**
>
> Si vous chargez une distribution que vous utilisez déjà pour distribuer le contenu, n'ajoutez des utilisateurs de confiance que lorsque vous êtes prêt à démarrer la génération d'URL signées pour vos objets. Après que vous avez ajouté les utilisateurs de confiance à une distribution, les utilisateurs doivent employer les URL signées pour accéder à un objet qui correspond à la valeur de `PathPattern` pour ce comportement de cache.

Compte AWS nombres

Ce paramètre s'applique uniquement lorsque vous choisissez Spécifier des comptes pour Signataires autorisés.

Si vous souhaitez créer des URL signées Comptes AWS en plus ou à la place du compte courant, entrez un Compte AWS chiffre par ligne dans ce champ. Notez ce qui suit :

- Les comptes que vous spécifiez doivent avoir au moins une paire de clés CloudFront active. Pour plus d'informations, consultez Création de paires de clés pour vos signataires.
- Vous ne pouvez pas créer de paires de CloudFront clés pour les utilisateurs IAM. Vous ne pouvez donc pas utiliser les utilisateurs IAM comme signataires de confiance.
- Pour plus d'informations sur la façon d'obtenir le Compte AWS numéro d'un compte, voir Afficher les Compte AWS identifiants dans le Guide de référence Compte AWS de gestion.
- Si vous entrez le numéro de compte du compte courant, cochez CloudFront automatiquement la case Automatique et supprimez le numéro de compte de la liste des numéros de AWS compte.

Compresser des objets automatiquement

Si vous souhaitez CloudFront compresser automatiquement certains types de fichiers lorsque les utilisateurs acceptent le contenu compressé, choisissez Oui. Quand CloudFront compresse votre contenu, les téléchargements sont beaucoup plus rapides, parce que les fichiers sont plus petits et que vos pages web s'affichent plus rapidement pour vos utilisateurs. Pour plus d'informations, consultez Diffusion de fichiers compressés.

CloudFront événement

Ce paramètre s'applique aux Associations de fonctions Lambda.

Vous pouvez choisir d'exécuter une fonction Lambda lorsqu'un ou plusieurs des CloudFront événements suivants se produisent :

- Quand CloudFront reçoit une demande d'un téléspectateur (demande du téléspectateur)
- Avant CloudFront de transmettre une demande à l'origine (demande d'origine)
- Quand CloudFront reçoit une réponse de l'origine (réponse d'origine)
- Before CloudFront renvoie la réponse au spectateur (réponse du spectateur)

Pour plus d'informations, consultez Choix de l'événement qui déclenche la fonction.

ARN de fonction Lambda

Ce paramètre s'applique aux Associations de fonctions Lambda.

Spécifiez l'Amazon Resource Name (ARN) de la fonction Lambda pour laquelle vous voulez ajouter un déclencheur. Pour savoir comment obtenir l'ARN d'une fonction, reportez-vous à l'étape 1 de la procédure Ajouter des déclencheurs à l'aide de la CloudFront console.

Inclure le corps

Ce paramètre s'applique aux Associations de fonctions Lambda.

Pour plus d'informations, consultez Inclure le corps.

Paramètres de distribution

Les valeurs suivantes s'appliquent à la totalité de la distribution.

Rubriques

- Catégorie de tarifs
- AWS WAF ACL web
- Noms de domaine alternatifs (CNAME)
- Certificat SSL
- Prise en charge d'un client SSL personnalisé
- Politique de sécurité (SSL/TLS version minimale)
- Versions de HTTP prises en charge
- Objet racine par défaut
- Journalisation standard
- Journaux de connexion.
- Préfixe de journal
- Journalisation des cookies
- Activation d'IPv6 (demandes des utilisateurs)
- Authentification mutuelle
- Activation d'IPv6 pour les origines personnalisées (demandes d'origine)
- Comment
- État de la distribution

Catégorie de tarifs

Choisissez la classe de prix qui correspond au prix maximum que vous souhaitez payer pour le CloudFront service. Par défaut, CloudFront diffuse vos objets à partir d'emplacements périphériques dans toutes les CloudFront régions.

Pour plus d'informations sur les classes de prix et sur l'impact de votre choix sur les CloudFront performances de votre distribution, consultez la section CloudFront Tarification.

AWS WAF ACL web

Vous pouvez protéger votre CloudFront distribution à l'aide AWS WAFd'un pare-feu d'applications Web qui vous permet de sécuriser vos applications Web et d'API afin de bloquer les demandes avant

qu'elles n'atteignent vos serveurs. Vous pouvez le faire Enable AWS WAF pour les distributions lors de la création ou de la modification d'une CloudFront distribution.

Vous pouvez éventuellement configurer ultérieurement des protections de sécurité supplémentaires pour d'autres menaces spécifiques à votre application dans la AWS WAF console à l'adresse https://console.aws.amazon.com/wafv2/.

Pour plus d'informations AWS WAF, consultez le guide du AWS WAF développeur.

Noms de domaine alternatifs (CNAME)

Facultatif. Spécifiez un ou plusieurs noms de domaine que vous souhaitez utiliser pour les URL de vos objets au lieu du nom de domaine attribué lors de CloudFront la création de votre distribution. Vous devez être propriétaire du nom de domaine ou être autorisé à l'utiliser, ce que vous devez vérifier en ajoutant un SSL/TLS certificat.

Par exemple, si vous voulez que l'URL de l'objet :

`/images/image.jpg`

se présente ainsi :

`https://www.example.com/images/image.jpg`

et non comme suit :

`https://d111111abcdef8.cloudfront.net/images/image.jpg`

Ajoutez un CNAME pour `www.example.com`.

> **Important**
>
> Si vous ajoutez un CNAME pour `www.example.com` à votre distribution, vous devez également effectuer les opérations suivantes :
>
> - Créez (ou mettez à jour) un enregistrement CNAME avec votre service DNS pour acheminer les requêtes de `www.example.com` vers `d111111abcdef8.cloudfront.net`.
> - Ajoutez un certificat CloudFront auprès d'une autorité de certification (CA) approuvée qui couvre le nom de domaine (CNAME) que vous ajoutez à votre distribution, afin de valider votre autorisation d'utiliser le nom de domaine.

Vous devez avoir l'autorisation de créer un enregistrement CNAME avec le fournisseur de services DNS du domaine. Cela signifie normalement que le domaine vous appartient ou que vous développez une application pour le propriétaire du domaine.

Pour connaître le nombre maximum actuel de noms de domaine alternatifs que vous pouvez ajouter à une distribution ou demander un quota plus élevé (auparavant appelé limite), consultez Quotas généraux sur les distributions.

Pour plus d'informations sur les noms de domaine alternatifs, consultez Utilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME). Pour plus d'informations sur CloudFront les URL, consultezPersonnalisez le format d'URL pour les fichiers dans CloudFront.

Certificat SSL

Si vous avez spécifié un nom de domaine alternatif à utiliser avec votre distribution, choisissez Certificat SSL personnalisé, puis, pour valider votre autorisation d'utiliser le nom de domaine alternatif, choisissez un certificat qui couvre cela. Pour que vos utilisateurs utilisent HTTPS pour accéder à vos objets, sélectionnez la valeur applicable.

- CloudFront Certificat par défaut (*.cloudfront.net) : choisissez cette option si vous souhaitez utiliser le nom de CloudFront domaine dans les URL de vos objets, tels que. `https://d111111abcdef8.cloudfront.net/image1.jpg`
- Certificat SSL personnalisé : choisissez cette option si vous souhaitez utiliser votre propre nom de domaine dans les URL de vos objets en tant que nom de domaine alternatif, tel que `https://example.com/image1.jpg`. Ensuite, choisissez un certificat à utiliser qui couvre le nom de domaine alternatif. La liste des certificats peut inclure l'un des éléments suivants :
  - Certificats fournis par AWS Certificate Manager
  - Les certificats que vous avez achetés auprès d'une autorité de certification tierce et chargés dans ACM
  - Les certificats que vous avez achetés auprès d'une autorité de certification tierce et chargés dans le magasin de certificats IAM

  Si vous choisissez cette valeur, il est recommandé de n'utiliser qu'un nom de domaine alternatif dans vos URL d'objet (https://example.com/logo.jpg). Si vous utilisez votre nom de domaine de CloudFront distribution (https://d111111abcdef8.cloudfront.net/logo.jpg) et qu'un client utilise un

ancien visualiseur qui ne prend pas en charge le SNI, la façon dont le lecteur réagit dépend de la valeur que vous avez choisie pour Clients pris en charge :

- Tous les clients : le lecteur affiche un avertissement car le nom de CloudFront domaine ne correspond pas au nom de domaine indiqué dans votre SSL/TLS certificat.
- Uniquement les clients qui supportent l'indication du nom du serveur (SNI) : CloudFront abandonne la connexion avec le visualiseur sans renvoyer l'objet.

Prise en charge d’un client SSL personnalisé

S’applique uniquement lorsque vous choisissez Certificat SSL personnalisé (exemple.com) pour Certificat SSL. Si vous avez indiqué un ou plusieurs noms de domaine alternatifs et un certificat SSL personnalisé pour la distribution, choisissez la manière dont vous CloudFront souhaitez traiter les requêtes HTTPS :

- Clients prenant en charge l’indication de nom de serveur (SNI, Server Name Indication) – (recommandé) : avec ce paramètre, pratiquement tous les navigateurs et clients web modernes peuvent se connecter à la distribution, car ils prennent en charge SNI. Cependant, certains utilisateurs peuvent utiliser d’anciens navigateurs web ou clients qui ne prennent pas en charge SNI, ce qui signifie qu’ils ne peuvent pas se connecter à la distribution.

  Pour appliquer ce paramètre à l'aide de l' CloudFront API, spécifiez-le `sni-only` dans le `SSLSupportMethod` champ. Dans CloudFormation, le champ est nommé `SslSupportMethod` (notez les différentes majuscules).
- Support des clients hérités : avec ce paramètre, les anciens navigateurs web et clients qui ne prennent pas en charge SNI peuvent se connecter à la distribution. Toutefois, ce paramètre entraîne des frais mensuels supplémentaires. Pour connaître le prix exact, rendez-vous sur la page CloudFront des tarifs d'Amazon et recherchez le SSL personnalisé sur la page Dedicated IP.

  Pour appliquer ce paramètre à l'aide de l' CloudFront API, spécifiez-le `vip` dans le `SSLSupportMethod` champ. Dans CloudFormation, le champ est nommé `SslSupportMethod` (notez les différentes majuscules).

Pour plus d’informations, consultez Choisissez la manière dont CloudFront les requêtes HTTPS sont traitées.

Politique de sécurité (SSL/TLS version minimale)

Spécifiez la politique de sécurité que vous CloudFront souhaitez utiliser pour les connexions HTTPS avec les spectateurs (clients). Une politique de sécurité détermine deux paramètres :

- SSL/TLS Protocole minimal CloudFront utilisé pour communiquer avec les spectateurs.
- Les chiffrements qui CloudFront peuvent être utilisés pour chiffrer le contenu renvoyé aux spectateurs.

Pour plus d'informations sur les politiques de sécurité, y compris les protocoles et les chiffrements inclus dans chacune d'elles, consultez Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront.

Les politiques de sécurité disponibles dépendent des valeurs que vous spécifiez pour le certificat SSL et le support client SSL personnalisé (connu sous le nom `CloudFrontDefaultCertificate` et `SSLSupportMethod` dans l' CloudFront API) :

- Lorsque le certificat SSL est le CloudFront certificat par défaut (*.cloudfront.net) (lorsqu'il `CloudFrontDefaultCertificate` se trouve `true` dans l'API), définit CloudFront automatiquement la politique de sécurité sur TLSv1.
- Lorsque Certificat SSL est Certificat SSL personnalisé (example.com) et que Prise en charge d'un client SSL personnalisé est Clients qui prennent en charge l'indication de nom de serveur (SNI) - (Recommandé) (lorsque `CloudFrontDefaultCertificate` est `false` et que `SSLSupportMethod` est `sni-only` dans l'API), vous pouvez choisir parmi les politiques de sécurité suivantes :
  - TLSv1.3_2025
  - TLSv1.2_2025
  - TLSv1.2_2021
  - TLSv1.2_2019
  - TLSv1.2_2018
  - TLSv1.1_2016
  - TLSv1_2016
  - TLSv1
- Lorsque Certificat SSL est SSL personnalisé (example.com) et que Prise en charge d'un client SSL personnalisé est Prise en charge de clients hérités (lorsque `CloudFrontDefaultCertificate`

est `false` et que `SSLSupportMethod` est `vip` dans l'API), vous pouvez choisir parmi les politiques de sécurité suivantes :

- TLSv1
- SSLv3

Dans cette configuration, les politiques de sécurité TLSv1.3 _2025, TLSv1.2 _2025, TLSv1.2 _2021, TLSv1.2 _2019, TLSv1.2 _2018, TLSv1.1 _2016 et TLSv1_2016 ne sont pas disponibles dans la console ou dans l'API. CloudFront Si vous souhaitez utiliser l'une de ces politiques de sécurité, vous disposez des options suivantes :

- Évaluez si votre distribution a besoin d'une prise en charge de client hérité avec adresses IP dédiées. Si vos utilisateurs prennent en charge l'indication de nom de serveur (SNI), nous vous recommandons de mettre à jour le paramètre Prise en charge d'un client SSL personnalisé de votre distribution sur Clients qui prennent en charge l'indication de nom de serveur (SNI) (définissez `SSLSupportMethod` sur `sni-only` dans l'API). Cela vous permet d'utiliser n'importe laquelle des politiques de sécurité TLS disponibles, et cela peut également réduire vos CloudFront frais.
- Si vous devez conserver le support des anciens clients avec des adresses IP dédiées, vous pouvez demander l'une des autres politiques de sécurité TLS (TLSv1.3_2025, _2025, TLSv1.2 TLSv1.2 _2021, TLSv1.2 _2019, TLSv1.2 _2018, TLSv1.1 _2016 ou TLSv1_2016) en créant un dossier dans le centre de support.AWS

  > **Note**
  >
  > Avant de contacter le AWS Support pour demander cette modification, prenez en compte les points suivants :
  >
  > - Lorsque vous ajoutez l'une de ces politiques de sécurité (TLSv1.3_2025, _2025, TLSv1.2 TLSv1.2 _2021, TLSv1.2 _2019, TLSv1.2 _2018, _2016 ou TLSv1.1 TLSv1_2016) à une distribution d'assistance aux anciens clients, la politique de sécurité est appliquée à toutes les demandes des utilisateurs n'appartenant pas au SNI pour toutes les distributions d'assistance aux anciens clients de votre compte. AWS Toutefois, lorsque les visionneuses envoient des demandes SNI à une distribution avec prise en charge de client hérité, la politique de sécurité de cette distribution s'applique. Pour vous assurer que la politique de sécurité souhaitée est appliquée à toutes les demandes des utilisateurs envoyées à toutes les distributions Legacy Clients Support de votre AWS compte, ajoutez la politique de sécurité souhaitée à chaque distribution individuellement.

- Par définition, la nouvelle politique de sécurité ne prend pas en charge les mêmes chiffrements et protocoles que l'ancienne. Par exemple, si vous choisissez de mettre à niveau la politique de sécurité d'une distribution de TLSv1 à TLSv1.1 _2016, cette distribution ne prendra plus en charge le chiffrement. DES-CBC3-SHA Pour plus d'informations sur les chiffrements et les protocoles pris en charge par chaque politique de sécurité, consultez Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront.

Versions de HTTP prises en charge

Choisissez les versions HTTP que vous souhaitez que votre distribution prenne en charge lorsque les utilisateurs communiquent avec elles CloudFront.

Pour les spectateurs et CloudFront pour l'utilisation HTTP/2, les utilisateurs doivent prendre en charge TLSv1.2 ou version ultérieure, et l'indication du nom du serveur (SNI).

Pour les spectateurs et CloudFront pour l'utilisation HTTP/3, les utilisateurs doivent prendre en charge TLSv1.3 l'indication du nom du serveur (SNI). CloudFront prend en charge la migration des HTTP/3 connexions pour permettre au spectateur de changer de réseau sans perdre la connexion. Pour plus d'informations sur la migration des connexions à distance, consultez Migration des connexions au RFC 9000.

> **Note**
>
> Pour plus d'informations sur les TLSv1.3 chiffrements pris en charge, consultez. Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront

> **Note**
>
> Si vous utilisez Amazon Route 53, vous pouvez utiliser des enregistrements HTTPS pour autoriser la négociation de protocole lors de la recherche DNS si le client le prend en charge. Pour plus d'informations, consultez Create alias resource record set.

Objet racine par défaut

Facultatif. L'objet que vous souhaitez demander CloudFront à votre origine (par exemple,`index.html`) lorsqu'un utilisateur demande l'URL racine de votre distribution (`https://www.example.com/`) au lieu d'un objet de votre distribution (`https://www.example.com/product-description.html`). Spécifier un objet racine par défaut permet d'éviter d'exposer le contenu de votre distribution.

La longueur maximale du nom est de 255 caractères. Le nom peut contenir l'un des caractères suivants :

- A-Z, a-z
- 0-9
- _ - . * $ / ~ " '
- &, transmis et renvoyé comme `&`

Lorsque vous spécifiez l'objet racine par défaut, entrez uniquement le nom de l'objet, par exemple, `index.html`. N'ajoutez pas `/` devant le nom de l'objet.

Pour plus d'informations, consultez Spécification d'un objet racine par défaut.

Journalisation standard

Spécifiez si vous CloudFront souhaitez enregistrer les informations relatives à chaque demande d'objet et stocker les fichiers journaux. Vous pouvez activer ou désactiver la journalisation à tout moment. L'activation de la journalisation n'entraîne aucun frais supplémentaire, toutefois vous pouvez encourir des coûts liés au stockage et à la consultation des fichiers. Vous pouvez supprimer les fichiers journaux à tout moment.

CloudFront prend en charge les options de journalisation standard suivantes :

- Journalisation standard (v2) — Vous pouvez envoyer des journaux vers des destinations de livraison, notamment Amazon CloudWatch Logs, Amazon Data Firehose et Amazon Simple Storage Service (Amazon S3).
- Journalisation standard (héritée) : vous ne pouvez envoyer des journaux que vers un compartiment Amazon S3.

Journaux de connexion.

Lorsque vous activez l'authentification mutuelle pour votre distribution, CloudFront fournit des journaux de connexion qui capturent les attributs relatifs aux demandes envoyées à vos distributions. Les journaux de connexion contiennent des informations telles que l'adresse IP et le port du client, les informations du certificat client, les résultats de la connexion et les chiffrements TLS utilisés. Ces journaux de connexion peuvent ensuite être utilisés pour examiner les modèles de demandes et d'autres tendances.

Pour en savoir plus sur les journaux de connexion, consultezObservabilité à l'aide des journaux de connexion.

Préfixe de journal

(Facultatif) Si vous activez la journalisation standard (ancienne), spécifiez la chaîne, le cas échéant, que vous CloudFront souhaitez préfixer aux noms des fichiers journaux d'accès pour cette distribution, par exemple,`exampleprefix/`. La barre oblique de fin (/) est facultative, mais recommandée pour simplifier la navigation dans vos fichiers-journaux. Pour plus d’informations, consultez Configurer la journalisation standard (héritée).

Journalisation des cookies

Si vous CloudFront souhaitez inclure des cookies dans les journaux d'accès, choisissez Activé. Si vous choisissez d'inclure des cookies dans les CloudFront journaux, enregistre tous les cookies, quelle que soit la manière dont vous configurez les comportements de cache pour cette distribution : transférer tous les cookies, ne transférer aucun cookie ou transmettre une liste spécifiée de cookies à l'origine.

Comme Amazon S3 ne traite pas les cookies, à moins que votre distribution n’inclue aussi une origine Amazon EC2 ou autre origine personnalisée, nous vous recommandons de choisir Off (Désactivé) comme valeur de Cookie Logging (Journalisation des cookies).

Pour plus d’informations sur les cookies, consultez Mise en cache de contenu basée sur des cookies.

Activation d’IPv6 (demandes des utilisateurs)

Si vous souhaitez répondre CloudFront aux demandes des utilisateurs provenant d'adresses IP IPv4 et IPv6, sélectionnez Activer IPv6. Pour plus d’informations, consultez Activer IPv6 pour les CloudFront distributions.

Authentification mutuelle

Facultatif. Vous pouvez choisir d'activer l'authentification mutuelle pour votre CloudFront distribution. Pour plus d’informations, consultez Authentification TLS mutuelle avec CloudFront (Viewer MTLS).

Activation d’IPv6 pour les origines personnalisées (demandes d’origine)

Lorsque vous utilisez une origine personnalisée (à l'exception des origines Amazon S3 et VPC), vous pouvez personnaliser les paramètres d'origine de votre distribution afin de choisir le mode de connexion à votre CloudFront origine à l'aide d'adresses IPv4 ou IPv6. Pour plus d’informations, consultez Activer IPv6 pour les CloudFront distributions.

Comment

Facultatif. Lorsque vous créez une distribution, vous pouvez inclure un commentaire de 128 caractères au plus. Vous pouvez mettre à jour le commentaire à tout moment.

État de la distribution

Indique si vous souhaitez que la distribution soit activée ou désactivée après son déploiement :

- Activé signifie que dès que la distribution est entièrement déployée, vous pouvez déployer les liens qui utilisent le nom de domaine de la distribution et que les utilisateurs peuvent extraire le contenu. Chaque fois qu'une distribution est activée, CloudFront accepte et gère toutes les demandes de contenu de l'utilisateur final qui emploient le nom de domaine associé à cette distribution.

  Lorsque vous créez, modifiez ou supprimez une CloudFront distribution, la propagation des modifications dans la CloudFront base de données prend du temps. Une demande immédiate d’informations sur une distribution peut ne pas afficher la modification. La propagation s’effectue généralement en quelques minutes, mais une charge système ou une partition du réseau élevées peuvent augmenter cette durée.
- Désactivé signifie que même si la distribution peut être déployée et prête à être utilisée, les utilisateurs ne peuvent pas l’utiliser. Chaque fois qu'une distribution est désactivée, CloudFront n'accepte aucune demande d'utilisateur final utilisant le nom de domaine associé à cette distribution. Tant que vous n’avez pas basculé la distribution de « disabled » en « enabled » (en mettant à jour la configuration de la distribution), personne ne peut l’utiliser.

Vous pouvez basculer une distribution de désactivée à activée (et inversement) aussi souvent que vous le voulez. Suivez la procédure de mise à jour de la configuration d'une distribution. Pour plus d'informations, consultez Mettre à jour une distribution.

Pages d'erreur personnalisées et mise en cache des erreurs

Vous pouvez avoir CloudFront renvoyé un objet au lecteur (par exemple, un fichier HTML) lorsque votre Amazon S3 ou votre origine personnalisée renvoie un code de statut HTTP 4xx ou 5xx à. CloudFront Vous pouvez également spécifier la durée pendant laquelle une réponse d'erreur provenant de votre origine ou d'une page d'erreur personnalisée est mise en cache dans les CloudFront caches périphériques. Pour plus d'informations, consultez Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques.

> **Note**
>
> Comme les valeurs suivantes ne sont pas incluses dans l'Assistant Create Distribution, vous ne pouvez configurer les pages d'erreur personnalisées que lorsque vous mettez à jour une distribution.

Rubriques

- Code d'erreur HTTP
- Chemin de la page de réponse
- Code de réponse HTTP
- Erreur de mise en cache de TTL minimum (secondes)

Code d'erreur HTTP

Code d'état HTTP pour lequel vous souhaitez CloudFront renvoyer une page d'erreur personnalisée. Vous pouvez configurer CloudFront pour renvoyer des pages d'erreur personnalisées pour aucun, certains ou tous les codes d'état HTTP mis en CloudFront cache.

Chemin de la page de réponse

Chemin d'accès à la page d'erreur personnalisée (par exemple, `/4xx-errors/403-forbidden.html`) que CloudFront doit renvoyer à un navigateur quand votre origine retourne

le code de statut HTTP que vous avez spécifié pour Code d'erreur (par exemple, 403). Si vous souhaitez stocker vos objets et vos pages d'erreur personnalisées dans des emplacements différents, votre distribution doit inclure un comportement de cache pour lequel les conditions suivantes sont vraies :

- La valeur de Modèle de chemin correspond au chemin d'accès de vos messages d'erreur personnalisés. Par exemple, supposons que vous ayez enregistré des pages d'erreur personnalisées pour les erreurs 4xx dans un compartiment Amazon S3 d'un répertoire nommé `/4xx-errors`. Votre distribution doit inclure un comportement de cache pour lequel le modèle de chemin transmet les demandes de vos pages d'erreur personnalisées vers cet emplacement, par exemple, /erreurs-4xx/*.
- La valeur d'Origine spécifie la valeur d'ID d'origine pour l'origine qui contient vos pages d'erreur personnalisées.

Code de réponse HTTP

Le code d'état HTTP que vous CloudFront souhaitez renvoyer au visualiseur avec la page d'erreur personnalisée.

Erreur de mise en cache de TTL minimum (secondes)

Durée minimale pendant laquelle vous souhaitez mettre en cache CloudFront les réponses aux erreurs depuis votre serveur d'origine.

Restrictions géographiques

Si vous devez empêcher les utilisateurs de certains pays d'accéder à votre contenu, vous pouvez configurer votre CloudFront distribution avec une liste d'autorisation ou une liste de blocage. Il n'y a pas de frais supplémentaires pour la configuration de restrictions géographiques. Pour plus d'informations, consultez Restriction de la distribution géographique de votre contenu.

Test d'une distribution

Une fois que vous avez créé votre distribution, CloudFront vous savez où se trouve votre serveur d'origine et vous connaissez le nom de domaine associé à la distribution. Pour tester votre distribution, procédez comme suit :

1. Attendez que votre distribution soit déployée.

- Consultez les Détails de votre distribution dans la console. Lorsque le déploiement de votre distribution est terminé, le champ Dernière modification passe de Déploiement à une date et une heure.

2. Créez des liens vers vos objets avec le nom de CloudFront domaine en suivant la procédure ci-dessous.
3. Testez les liens. CloudFront fournit les objets à votre page Web ou à votre application.

Création de liens vers vos objets

Utilisez la procédure suivante pour créer des liens de test pour les objets de votre distribution CloudFront Web.

Pour créer des liens aux objets dans une distribution web

1. Copiez le code HTML suivant dans un nouveau fichier, remplacez-le *domain-name* par le nom de domaine de votre distribution et remplacez-le *object-name* par le nom de votre objet.

```
<html>
<head>
 <title>My CloudFront Test</title>
</head>
<body>
 <p>My text content goes here.</p>
 <p><img src="https://domain-name/object-name" alt="my test image"></p>
</body>
</html>
```

   Par exemple, si votre nom de domaine était `d111111abcdef8.cloudfront.net` et que votre objet était `image.jpg`, l'URL du lien sera :

   `https://d111111abcdef8.cloudfront.net/image.jpg`.

   Si votre objet se trouve dans un dossier de votre serveur d'origine, le dossier doit également être inclus dans l'URL. Par exemple, si image.jpg se trouvait dans le dossier images de votre serveur d'origine, l'URL serait :

   `https://d111111abcdef8.cloudfront.net/images/image.jpg`

2. Enregistrez le code HTML dans un fichier ayant .html comme extension de nom de fichier.

3. Ouvrez votre page Web dans un navigateur pour vous assurer que vous pouvez voir votre objet.

Le navigateur renvoie votre page avec le fichier image intégré, diffusé à partir de l'emplacement périphérique qui a été CloudFront déterminé comme approprié pour servir l'objet.

Mettre à jour une distribution

Dans la CloudFront console, vous pouvez voir les CloudFront distributions associées à votre Compte AWS, consulter les paramètres d'une distribution et mettre à jour la plupart des paramètres. Sachez que les modifications que vous apportez aux paramètres ne prennent effet qu'après propagation de la distribution aux emplacements périphériques AWS .

Mise à jour d'une distribution dans la console

Les procédures suivantes indiquent comment mettre à jour une CloudFront distribution dans la console.

Multi-tenant

Pour mettre à jour une distribution multi-locataires

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Recherchez et choisissez l'ID de la distribution multi-locataires.
3. Choisissez l'onglet correspondant aux paramètres que vous souhaitez mettre à jour.
4. Apportez les mises à jour souhaitées puis, pour enregistrer vos modifications, choisissez Enregistrer les modifications. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez Référence des paramètres de distribution préconfigurés.

Vous pouvez également mettre à jour une distribution à l'aide de l' CloudFront API :

- Pour mettre à jour une distribution, consultez UpdateDistributionle Amazon CloudFront API Reference.

> **Important**
>
> Lors de la mise à jour d'une distribution, sachez que vous devrez renseigner des champs qui ne sont pas exigés lors de sa création. Pour vous assurer que tous les champs obligatoires sont inclus lorsque vous utilisez l' CloudFront API pour mettre à jour une distribution, suivez les étapes décrites UpdateDistributiondans le manuel Amazon CloudFront API Reference.

Pour modifier la configuration multi-locataires d'un locataire de distribution, mettez à jour ce locataire de distribution. Vous mettez également à jour le locataire de distribution pour mettre à jour son domaine, son certificat, ses personnalisations ou ses valeurs de paramètres. Pour plus de détails sur la mise à jour du certificat du locataire de distribution, consultez Ajout d'un domaine et d'un certificat (locataire de distribution).

Pour mettre à jour un locataire de distribution

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans SaaS, choisissez Locataires de distribution.
3. Recherchez le locataire de distribution. Utilisez le menu déroulant de la barre de recherche pour filtrer par domaine, nom, ID de distribution, ID de certificat, ID de groupe de connexions ou ID de liste ACL web.
4. Choisissez le nom du locataire de distribution.
5. Pour mettre à jour les Détails généraux, choisissez Modifier, effectuez les mises à jour, puis sélectionnez Mettre à jour le locataire de distribution.
6. Choisissez l'onglet approprié pour tous les autres paramètres à mettre à jour, effectuez vos modifications et enregistrez-les. Pour plus d'informations sur les paramètres des locataires de distribution que vous pouvez personnaliser, consultez Personnalisations du locataire de distribution.

Standard

Pour mettre à jour une distribution standard

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

2. Sélectionnez l'ID d'une distribution. La liste inclut toutes les distributions associées au AWS compte que vous avez utilisé pour vous connecter à la CloudFront console.
3. Pour mettre à jour les paramètres généraux, choisissez Modifier. Sinon, choisissez l'onglet correspondant aux paramètres que vous souhaitez mettre à jour.
4. Apportez les modifications souhaitées, puis choisissez Enregistrer les modifications. Pour plus d'informations sur les champs, consultez les rubriques suivantes :
   - Paramètres généraux : Paramètres de distribution
   - Paramètres d'origine : Paramètres d'origine
   - Paramètres de comportement du cache : Paramètres de comportement du cache
5. Pour supprimer une origine de votre distribution, procédez comme suit :
   a. Choisissez Comportements et assurez-vous d'avoir déplacé tous les comportements de cache par défaut associés à l'origine vers une autre origine.
   b. Choisissez Origines, puis sélectionnez une origine.
   c. Sélectionnez Supprimer.

Vous pouvez également mettre à jour une distribution à l'aide de l' CloudFront API :

- Pour mettre à jour une distribution, consultez UpdateDistributionle Amazon CloudFront API Reference.

> **Important**
>
> Lorsque vous mettez à jour votre distribution, sachez qu'un certain nombre de champs supplémentaires sont requis qui ne sont pas nécessaires pour créer une distribution. Pour vous assurer que tous les champs obligatoires sont inclus lorsque vous utilisez l' CloudFront API pour mettre à jour une distribution, suivez les étapes décrites UpdateDistributiondans le manuel Amazon CloudFront API Reference.

Lorsque vous enregistrez les modifications apportées à votre configuration de distribution, les modifications CloudFront commencent à être propagées à tous les emplacements périphériques. Les modifications de configuration successives se propagent dans leur ordre respectif. Tant que votre configuration n'est pas mise à jour dans un emplacement périphérique, CloudFront continue

de diffuser votre contenu à partir de cet emplacement sur la base de la configuration précédente. Une fois votre configuration mise à jour dans un emplacement périphérique, CloudFront commence immédiatement à diffuser votre contenu à partir de cet emplacement sur la base de la nouvelle configuration.

Vos modifications ne se propagent pas simultanément vers chaque emplacement périphérique. Lors CloudFront de la propagation de vos modifications, nous ne pouvons pas déterminer si un emplacement périphérique donné diffuse votre contenu en fonction de la configuration précédente ou de la nouvelle configuration.

> **Note**
>
> Dans de rares cas, lorsqu'un hôte ou un lien réseau est perturbé, une partie du trafic du locataire de distribution peut être servie avec d'anciennes configurations pendant une courte période, jusqu'à ce que vos modifications se propagent dans le réseau.

Pour savoir quand vos modifications sont propagées, consultez les Détails de votre distribution dans la console. Lorsque le déploiement est terminé, le champ Dernière modification passe de Déploiement à une date et une heure.

Marquer une CloudFront ressource

Les balises sont des mots ou des phrases que vous pouvez utiliser pour identifier et organiser vos AWS ressources. Vous pouvez ajouter plusieurs balises à une ressource, chacune de ces balises étant composée d'une clé et d'une valeur que vous définissez. Par exemple, vous pouvez choisir la clé « domaine » et la valeur « exemple.com ». Vous pouvez rechercher et filtrer vos ressources en fonction des balises que vous ajoutez. Pour plus d'informations sur les cas d'utilisation des balises, consultez la section Stratégies de balisage courantes dans le guide des AWS ressources de balisage et de l'éditeur de balises.

Vous pouvez utiliser des balises avec CloudFront, comme dans les exemples suivants :

- Appliquez des autorisations basées sur des balises sur les CloudFront distributions. Pour plus d'informations, consultez ABAC avec CloudFront.
- Suivre les informations de facturation dans différentes catégories. Lorsque vous appliquez des balises à des CloudFront distributions ou à d'autres AWS ressources (telles que des instances Amazon EC2 ou des compartiments Amazon S3) et que vous activez les balises, vous AWS

générez un rapport de répartition des coûts sous forme de valeur séparée par des virgules (fichier CSV) avec votre utilisation et vos coûts agrégés par vos balises actives.

Vous pouvez appliquer des balises associées à des catégories métier (telles que les centres de coûts, les noms d'applications ou les propriétaires) pour organiser les coûts relatifs à divers services. Pour en savoir plus sur l'utilisation des identifications pour la répartition des coûts, consultez Utilisation des identifications de répartition des coûts dans le Guide de l'utilisateur AWS Billing .

Remarques

- Vous pouvez appliquer des balises aux distributions, mais pas aux invalidations ni aux identités Origin Access Identity.
- L'éditeur de balises et les groupes de ressources ne sont actuellement pas pris en charge pourCloudFront.
- Pour connaître le nombre maximum de balises que vous pouvez actuellement ajouter à une distribution, consultez la page Quotas généraux.

Table des matières

- Restrictions liées aux étiquettes
- Baliser vos ressources pour facturation
- Ajouter, modifier et supprimer des balises
- Balisage par programmation

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises :

- Pour connaître le nombre maximal de balises par distribution, consultez Quotas généraux.
- Longueur de clé maximale : 128 caractères Unicode
- Longueur de valeur maximale : 256 caractères Unicode
- Valeurs valides pour la clé et la valeur : a-z A-Z, 0-9, espace et les caractères suivants : _. :/= + - et @

- Les clés et valeurs de balise sont sensibles à la casse
- N'utilisez pas `aws:` comme préfixe pour les clés. Ce préfixe est réservé à l'usage d' AWS .

Baliser vos ressources pour facturation

Vous pouvez utiliser des balises pour organiser votre AWS facture afin de refléter votre propre structure de coûts. Pour ce faire, vous devez d'abord activer les balises pour la répartition des coûts dans la console Billing and Cost Management. Pour plus d'informations sur la configuration d'un rapport de répartition des coûts avec des balises, voir Rapport de répartition des coûts mensuel dans le Guide AWS de l'utilisateur de facturation. Pour voir le coût de vos ressources combinées, vous pouvez organiser vos informations de facturation en fonction des ressources possédant les mêmes valeurs de clé d'étiquette. Par exemple, vous pouvez étiqueter plusieurs ressources avec un nom d'application spécifique, puis organiser vos informations de facturation pour afficher le coût total de cette application dans plusieurs services. Pour plus d'informations, consultez la section Utilisation des balises de répartition des coûts dans le Guide AWS de l'utilisateur de facturation.

> **Note**
>
> Si vous venez d'activer la création de rapports, les données du mois en cours peuvent être consultées après 24 heures.

Ajouter, modifier et supprimer des balises

Vous pouvez utiliser la CloudFront console pour gérer les balises associées à vos CloudFront ressources.

Pour ajouter des balises, modifier ou supprimer des balises pour une ressource

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Accédez à votre ressource :
   - Pour une distribution : choisissez l'ID de la distribution que vous souhaitez mettre à jour.
   - Pour une fonction : choisissez Fonctions, puis le nom de la fonction que vous souhaitez mettre à jour.

- Pour un KeyValueStore : Choisissez Fonctions, KeyValueStore cliquez sur l'onglet, puis choisissez le nom de la fonction KeyValueStore que vous souhaitez mettre à jour.

3. Sélectionnez l'onglet Tags (Identifications).
4. Choisissez Gérer les balises.
5. Sur la page de gestion des étiquettes, vous pouvez effectuer les opérations suivantes :
   - Pour ajouter une balise, renseignez une clé et, si nécessaire, une valeur. Choisissez Ajouter une nouvelle balise pour ajouter plus de balises.
   - Pour modifier une étiquette, modifiez la clé de l'étiquette, sa valeur ou les deux. Vous pouvez supprimer la valeur d'une étiquette, mais la clé est obligatoire.
   - Pour supprimer une balise, sélectionnez Remove (Supprimer).
6. Cliquez sur Enregistrer les modifications.

Balisage par programmation

Vous pouvez également utiliser l' CloudFront API AWS Command Line Interface (AWS CLI), AWS les SDK et AWS Tools for Windows PowerShell appliquer des balises. Pour plus d'informations, consultez les rubriques suivantes :

- CloudFront Opérations d'API :
  - ListTagsForResource
  - TagResource
  - UntagResource
- AWS CLI — Voir cloudfront dans le manuel de référence des AWS CLI commandes
- AWS SDK — Consultez la documentation du SDK applicable sur la page de AWS documentation
- Outils pour Windows PowerShell — Voir Amazon CloudFront dans le manuel de référence des Outils AWS pour PowerShell applets de commande

Supprimer une distribution

La procédure suivante supprime une distribution à l'aide de la CloudFront console. Pour plus d'informations sur la suppression à l'aide de l' CloudFront API, consultez DeleteDistributionle manuel Amazon CloudFront API Reference.

Si vous devez supprimer une distribution avec un OAC associé à un compartiment S3, consultez Suppression d'une distribution avec un OAC associé à un compartiment S3 pour connaître les points importants.

⚠ Warning

- Avant de pouvoir supprimer une distribution, vous devez la désactiver, ce qui nécessite l'autorisation de la mettre à jour. Une fois supprimée, une distribution ne peut pas être récupérée.
- Si vous désactivez une distribution associée à un autre nom de domaine, elle CloudFront cesse d'accepter du trafic pour ce nom de domaine (tel que www.exemple.com), même si une autre distribution possède un nom de domaine alternatif avec un caractère générique (*) correspondant au même domaine (par exemple *.exemple.com).
- Vous ne pouvez pas supprimer une distribution souscrite à un plan tarifaire CloudFront forfaitaire. Vous recevrez un message d'erreur indiquant : « Vous ne pouvez pas supprimer cette distribution tant qu'elle est souscrite à un plan tarifaire ». Vous devez d'abord annuler le plan tarifaire, puis, après le cycle de facturation en cours, supprimer la distribution.

Multi-tenant

Avant de supprimer une distribution multi-locataires, vous devez commencer par supprimer tous les locataires de distribution associés.

Pour supprimer une distribution multi-locataires

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet droit de la CloudFront console, choisissez le nom de la distribution multi-locataires que vous souhaitez supprimer.
3. Pour Locataires, sélectionnez et supprimez tous les locataires de distribution associés.
4. Choisissez Désactiver pour désactiver la distribution, puis sélectionnez Désactiver la distribution pour confirmer.
5. Attendez que le nouvel horodatage s'affiche dans la colonne Dernière modification.
   - La propagation de votre modification CloudFront à tous les emplacements périphériques peut prendre quelques minutes.

6. Choisissez Supprimer, Supprimer la distribution.

Pour supprimer un locataire de distribution

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans SaaS, choisissez Locataires de distribution.
3. Recherchez le locataire de distribution. Utilisez le menu déroulant de la barre de recherche pour filtrer par domaine, nom, ID de distribution, ID de certificat, ID de groupe de connexions ou ID de liste ACL web.
4. Sélectionnez le locataire de distribution à supprimer.
5. Choisissez Supprimer le locataire, Supprimer le locataire de distribution.

Standard

Pour supprimer une distribution standard

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet droit de la CloudFront console, recherchez la distribution que vous souhaitez supprimer.

   - Si la colonne État indique que la distribution est déjà Désactivée, passez à l’étape 6.
   - Si l’État indique Activé mais que la colonne Dernière modification affiche encore Déploiement, attendez la fin du déploiement avant de passer à l’étape 3.
3. Dans le volet droit de la CloudFront console, cochez la case correspondant à la distribution que vous souhaitez supprimer.
4. Choisissez Disable (Désactiver) pour désactiver la distribution, puis Yes, Disable (Oui, désactiver) pour confirmer. Sélectionnez ensuite Fermer.

   - La valeur de la colonne État change immédiatement en Désactivé.
5. Attendez que le nouvel horodatage s’affiche dans la colonne Dernière modification.

   - La propagation de votre modification CloudFront à tous les emplacements périphériques peut prendre quelques minutes.
6. Cochez la case correspondant à la distribution que vous souhaitez supprimer.

7. Choisissez Delete (Supprimer), Delete (Supprimer).

   - Si l'option Supprimer n'est pas disponible, cela signifie que CloudFront votre modification continue de se propager aux emplacements périphériques. Attendez que le nouvel horodatage s'affiche dans la colonne Dernière modification, puis répétez les étapes 6 à 7.

Utilisez différentes origines avec les CloudFront distributions

Lorsque vous créez une distribution, vous spécifiez l'origine à laquelle les demandes de fichiers sont CloudFront envoyées. Vous pouvez utiliser différents types d'origines avec CloudFront. Par exemple, vous pouvez utiliser un compartiment Amazon S3, un MediaStore conteneur, un MediaPackage canal, un Application Load Balancer ou une URL de AWS Lambda fonction. Lorsque vous créez votre CloudFront distribution, configure CloudFront automatiquement la plupart des paramètres de distribution pour vous, en fonction du type d'origine de votre contenu. Pour plus d'informations, consultez Référence des paramètres de distribution préconfigurés.

Si une instance Application Load Balancer, Network Load Balancer ou EC2 se trouve dans un sous-réseau privé, vous pouvez l'utiliser comme origine VPC. Avec les origines VPC, vos applications ne sont accessibles que dans un sous-réseau privé doté d'une CloudFront distribution, ce qui empêche l'accès de votre application sur l'Internet public. Pour plus d'informations, consultez the section called "Restriction de l'accès avec les origines de VPC".

> **Note**
>
> Vous pouvez utiliser les fonctions périphériques pour sélectionner dynamiquement l'origine appropriée pour chaque demande. À l'aide de CloudFront Functions ou de Lambda @Edge, vous pouvez acheminer les demandes vers différentes origines en fonction de facteurs tels que l'emplacement géographique du lecteur, les en-têtes des demandes ou les paramètres de chaîne de requête. Pour plus d'informations, consultez Personnalisation en périphérie à l'aide de fonctions.

Rubriques

- Utilisation d'un compartiment Amazon S3
- Utiliser un MediaStore conteneur ou un MediaPackage canal
- Utilisation d'un Application Load Balancer
- Utilisation d'un Network Load Balancer

- Utilisation d’une URL de fonction Lambda
- Utilisez un AWS Lambda Fonction Web
- Utilisation d’Amazon EC2 (ou autre origine personnalisée)
- Utiliser des groupes CloudFront d'origine
- Utilisation d’Amazon API Gateway

Utilisation d’un compartiment Amazon S3

Les rubriques suivantes décrivent les différentes manières d'utiliser un compartiment Amazon S3 comme origine d'une CloudFront distribution.

Rubriques

- Utilisation d’un compartiment Amazon S3 standard
- Utilisation d’Amazon S3 Object Lambda
- Utilisation d’un point d’accès Amazon S3
- Utilisation d’un compartiment Amazon S3 configuré en tant que point de terminaison de site web
- Ajouter CloudFront à un compartiment Amazon S3 existant
- Déplacer un compartiment Amazon S3 vers un autre Région AWS
- Utiliser un point d' Multi-Region accès Amazon S3

Utilisation d’un compartiment Amazon S3 standard

Lorsque vous utilisez Amazon S3 comme origine pour votre distribution, vous placez les objets que vous CloudFront souhaitez livrer dans un compartiment Amazon S3. Vous pouvez utiliser n’importe quelle méthode prise en charge par Amazon S3 pour accéder à vos objets dans Amazon S3. Par exemple, vous pouvez utiliser la console ou l'API Amazon S3, ou un outil tiers. Vous pouvez créer une hiérarchie dans votre compartiment pour stocker les objets, comme vous le feriez avec tout autre compartiment Amazon S3 standard.

L'utilisation d'un compartiment Amazon S3 existant comme serveur CloudFront d'origine ne modifie en rien le compartiment ; vous pouvez toujours l'utiliser comme vous le feriez normalement pour stocker et accéder à des objets Amazon S3 au prix standard d'Amazon S3. Le stockage d’objets dans le compartiment fait l’objet de frais Amazon S3 réguliers. Pour plus d'informations sur les frais d'utilisation CloudFront, consultez Amazon CloudFront Pricing. Pour plus d'informations sur

l'utilisation CloudFront avec un compartiment S3 existant, consultezthe section called “Ajouter CloudFront à un compartiment Amazon S3 existant”.

> **Important**
>
> Pour que votre bucket fonctionne CloudFront, le nom doit être conforme aux exigences de dénomination du DNS. Pour plus d’informations, consultez Règles de dénomination de compartiment dans le Guide de l’utilisateur Amazon Simple Storage Service.

Lorsque vous spécifiez un compartiment Amazon S3 comme origine pour CloudFront, nous vous recommandons d'utiliser le format suivant :

bucket-name.s3.*region*.amazonaws.com

Lorsque vous spécifiez le nom de compartiment dans ce format, vous pouvez utiliser les fonctions CloudFront suivantes :

- Configurez CloudFront pour communiquer avec votre compartiment Amazon S3 à l'aide de SSL/TLS. Pour plus d’informations, consultez the section called “Utilisez le protocole HTTPS avec CloudFront”.
- Utilisez un contrôle d'accès à l'origine pour obliger les spectateurs à accéder à votre contenu à l'aide d' CloudFrontURL, et non à l'aide d'URL Amazon S3. Pour plus d’informations, consultez the section called “Restriction de l’accès à une origine Amazon S3”.
- Mettez à jour le contenu de votre bucket en le soumettant POST et en faisant PUT des demandes à CloudFront. Pour plus d’informations, consultez the section called “Méthodes HTTP” dans la rubrique the section called “Comment CloudFront traiter et transférer les demandes vers votre origine Amazon S3”.

Ne spécifiez pas le compartiment à l’aide des formats suivants :

- Le type de chemin d’accès Amazon S3 : s3.amazonaws.com/*bucket-name*
- Le CNAME Amazon S3

> **Note**
>
> CloudFront prend en charge les origines S3 en utilisant n'importe quelle classe de stockage, y compris S3Intelligent-Tiering. Lorsque CloudFront des objets sont demandés depuis une origine S3, les objets sont récupérés quel que soit le niveau de stockage dans lequel ils se trouvent actuellement. L'utilisation CloudFront avec S3 Intelligent-Tiering n'a aucun impact sur les performances ou les fonctionnalités de votre distribution. Pour plus d'informations, consultez la section Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Utilisation d'Amazon S3 Object Lambda

Quand vous créez un point d'accès Object Lambda, Amazon S3 génère automatiquement un alias unique pour votre point d'accès Object Lambda. Vous pouvez utiliser cet alias au lieu d'un nom de compartiment Amazon S3 comme origine pour votre CloudFront distribution.

Lorsque vous utilisez un alias de point d'accès Object Lambda comme origine pour CloudFront, nous vous recommandons d'utiliser le format suivant :

alias.s3.*region*.amazonaws.com

Pour plus d'informations sur la manière de rechercher l'*alias*, consultez Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda de compartiment S3 dans le Guide de l'utilisateur Amazon S3.

> **Important**
>
> Lorsque vous utilisez un point d'accès Object Lambda comme origine pour CloudFront, vous devez utiliser le contrôle d'accès à l'origine.

Pour un exemple de cas d'utilisation, consultez Utiliser Amazon S3 Object Lambda avec Amazon pour adapter CloudFront le contenu aux utilisateurs finaux.

CloudFront traite l'origine d'un point d'accès Object Lambda de la même manière qu'une origine de compartiment Amazon S3 standard.

Si vous utilisez Amazon S3 Object Lambda comme origine pour votre distribution, vous devez configurer les quatre autorisations suivantes.

Object Lambda Access Point

Pour ajouter des autorisations pour le point d'accès Object Lambda

1. Connectez-vous à la console Amazon S3 Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation, choisissez Points d'accès Lambda d'objet.
3. Choisissez le point d'accès Object Lambda que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Stratégie de point d'accès Lambda d'objet.
6. Collez la politique suivante dans le champ Politique.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3-object-lambda:Get*",
            "Resource": "arn:aws:s3-object-lambda:us-
east-1:123456789012:accesspoint/Object-Lambda-Access-Point-name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/CloudFront-distribution-
ID"
                }
            }
        }
    ]
}
```

7. Cliquez sur Enregistrer les modifications.

Amazon S3 Access Point

Pour ajouter des autorisations pour le point d’accès Amazon S3

1. Connectez-vous à la console Amazon S3 Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation, choisissez Points d'accès.
3. Choisissez le point d'accès Amazon S3 que vous souhaitez utiliser.
4. Choisissez l’onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Stratégie de point d'accès.
6. Collez la politique suivante dans le champ Politique.

   JSON

```
{
    "Version":"2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name/object/*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "s3-object-lambda.amazonaws.com"
                }
            }
        }
    ]
}
```

7. Cliquez sur Enregistrer.

Amazon S3 bucket

Pour ajouter des autorisations au compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le compartiment Amazon S3 que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Politique de compartiment.
6. Collez la politique suivante dans le champ Politique.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:DataAccessPointAccount": "AWS-account-ID"
                }
            }
        }
    ]
}
```

7. Cliquez sur Enregistrer les modifications.

AWS Lambda function

Pour ajouter des autorisations à la fonction Lambda

1. Connectez-vous à la AWS Lambda console Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le volet de navigation, choisissez Fonctions.
3. Choisissez la AWS Lambda fonction que vous souhaitez utiliser.
4. Choisissez l'onglet Configuration, puis choisisssez Autorisations.
5. Choisissez Ajouter des autorisations dans la section des déclarations de Resource-based politique.
6. Sélectionnez Compte AWS.
7. Entrez un nom pour ID de déclaration.
8. Entrez `cloudfront.amazonaws.com` pour Principal.
9. Choisissez `lambda:InvokeFunction` dans le menu déroulant Action.
10. Cliquez sur Enregistrer.

Utilisation d’un point d’accès Amazon S3

Lorsque vous utilisez un point d’accès S3, Amazon S3 génère automatiquement un alias unique pour vous. Vous pouvez utiliser cet alias au lieu d'un nom de compartiment Amazon S3 comme origine pour votre CloudFront distribution.

Lorsque vous utilisez un alias de point d'accès Amazon S3 comme origine pour CloudFront, nous vous recommandons d'utiliser le format suivant :

alias.s3.*region*.amazonaws.com

Pour plus d’informations sur la manière de rechercher l’*alias*, consultez Utilisation d’un alias de type compartiment pour votre point d’accès de compartiment S3 dans le Guide de l’utilisateur Amazon S3.

> **Important**
>
> Lorsque vous utilisez un point d'accès Amazon S3 comme origine pour CloudFront, vous devez utiliser le contrôle d'accès à l'origine.

CloudFront traite l'origine d'un point d'accès Amazon S3 de la même manière qu'une origine de compartiment Amazon S3 standard.

Si vous utilisez Amazon S3 Object Lambda comme origine pour votre distribution, vous devez configurer les deux autorisations suivantes.

Amazon S3 Access Point

Pour ajouter des autorisations pour le point d'accès Amazon S3

1. Connectez-vous à la console Amazon S3 Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation, choisissez Points d'accès.
3. Choisissez le point d'accès Amazon S3 que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Stratégie de point d'accès.
6. Collez la politique suivante dans le champ Politique.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "s3objlambda",
            "Effect": "Allow",
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/Access-
Point-name/object/*"
            ],
            "Condition": {
                "StringEquals": {"aws:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/CloudFront-distribution-
ID"}
            }
```

```
        }
    ]
}
```

7. Cliquez sur Enregistrer.

Amazon S3 bucket

Pour ajouter des autorisations au compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le compartiment Amazon S3 que vous souhaitez utiliser.
4. Choisissez l'onglet Permissions (Autorisations).
5. Choisissez Modifier dans la section Politique de compartiment.
6. Collez la politique suivante dans le champ Politique.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": "*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:DataAccessPointAccount": "AWS-account-ID"
                }
            }
        }
    ]
```

```
}
```

7. Cliquez sur Enregistrer les modifications.

Utilisation d'un compartiment Amazon S3 configuré en tant que point de terminaison de site web

Vous pouvez utiliser un compartiment Amazon S3 configuré comme point de terminaison de site Web comme origine personnalisée avecCloudFront. Lorsque vous configurez votre CloudFront distribution, pour l'origine, entrez le point de terminaison d'hébergement de site Web statique Amazon S3 pour votre compartiment. La valeur s'affiche dans la console Amazon S3, sur l'onglet Properties (Propriétés), dans le volet Static website hosting (Hébergement de site Web statique). Par exemple :

`http://bucket-name.s3-website-region.amazonaws.com`

Pour plus d'informations sur la spécification de points de terminaison web statiques Amazon S3, consultez Points de terminaison de sites web dans le Guide de l'utilisateur Amazon Simple Storage Service.

Lorsque vous spécifiez le nom du compartiment dans ce format comme votre origine, vous pouvez utiliser les redirections Amazon S3 et les documents d'erreur personnalisés Amazon S3. Pour plus d'informations, consultez Configuration d'un document d'erreur personnalisé et Configuration d'une redirection dans le guide de l'utilisateur d'Amazon Simple Storage Service. (fournit CloudFront également des pages d'erreur personnalisées. Pour plus d'informations, voirthe section called "Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques".)

L'utilisation d'un compartiment Amazon S3 comme serveur CloudFront d'origine ne modifie en rien le compartiment. Vous pouvez continuer de l'utiliser normalement et des frais Amazon S3 réguliers s'appliquent. Pour plus d'informations sur les frais d'utilisation CloudFront, consultez Amazon CloudFront Pricing.

> **Note**
>
> Si vous utilisez l' CloudFront API pour créer votre distribution avec un compartiment Amazon S3 configuré comme point de terminaison de site Web, vous devez le configurer en utilisant`CustomOriginConfig`, même si le site Web est hébergé dans un compartiment Amazon S3. Pour plus d'informations sur la création de distributions à l'aide de l'CloudFront API, consultez CreateDistributionle Amazon CloudFront API Reference.

Ajouter CloudFront à un compartiment Amazon S3 existant

Si vous stockez vos objets dans un compartiment Amazon S3, vous pouvez soit demander aux utilisateurs d'obtenir vos objets directement auprès de S3, soit configurer CloudFront pour obtenir vos objets depuis S3, puis les distribuer à vos utilisateurs. L'utilisation CloudFront peut être plus rentable si vos utilisateurs accèdent fréquemment à vos objets car, en cas d'utilisation élevée, le prix du transfert de CloudFront données est inférieur à celui du transfert de données Amazon S3. De plus, les téléchargements sont plus rapides avec CloudFront Amazon S3 uniquement, car vos objets sont stockés plus près de vos utilisateurs.

> **Note**
>
> Si vous CloudFront souhaitez respecter les paramètres de partage de ressources entre origines d'Amazon S3, configurez CloudFront pour transmettre l'`Origin`en-tête à Amazon S3. Pour plus d'informations, consultez the section called "Mise en cache de contenu basée sur des en-têtes de demandes".

Si vous distribuez actuellement du contenu directement depuis votre compartiment Amazon S3 en utilisant votre propre nom de domaine (tel que example.com) au lieu du nom de domaine de votre compartiment Amazon S3 (tel que amzn-s3-demo-bucket. s3.us-west-2.amazonaws.com), vous pouvez l'ajouter CloudFront sans interruption en suivant la procédure suivante.

À ajouter CloudFront lorsque vous distribuez déjà votre contenu depuis Amazon S3

1. Créez une CloudFront distribution. Pour plus d'informations, consultez the section called "Créer une distribution".

   Lors de la création de la distribution, indiquez le nom de votre compartiment Amazon S3 comme serveur d'origine.

   > **Important**
   >
   > Pour que votre bucket fonctionne CloudFront, le nom doit être conforme aux exigences de dénomination du DNS. Pour plus d'informations, consultez Règles de dénomination de compartiment dans le Guide de l'utilisateur Amazon Simple Storage Service.

   Si vous utilisez un CNAME avec Amazon S3, indiquez aussi le CNAME de votre distribution.

2. Créez une page web test qui contient des liens vers des objets accessibles au public dans votre compartiment Amazon S3 et testez les liens. Pour ce test initial, utilisez le nom de domaine CloudFront de votre distribution dans les URL d'objets, comme par exemple, `https://d111111abcdef8.cloudfront.net/images/image.jpg`.

   Pour plus d'informations sur le format des CloudFront URL, consultezthe section called “Personnalisation des URL de fichier”.

3. Si vous utilisez des CNAME Amazon S3, votre application emploie votre nom de domaine (comme par exemple example.com) pour référencer les objets de votre compartiment Amazon S3 au lieu d’employer le nom de votre compartiment (comme par exemple amzn-s3-demo-bucket.s3.amazonaws.com). Pour continuer à utiliser votre nom de domaine pour référencer des objets au lieu d'utiliser le nom de CloudFront domaine de votre distribution (par exemple, d111111abcdef8.cloudfront.net), vous devez mettre à jour vos paramètres auprès de votre fournisseur de services DNS.

   Pour que les CNAME Amazon S3 fonctionnent, votre prestataire de services DNS doit disposer d’un jeu d’enregistrements de ressources CNAME pour votre domaine qui achemine actuellement les requêtes pour le domaine vers votre compartiment Amazon S3. Si un utilisateur demande, par exemple, cet objet :

   ```
   https://example.com/images/image.jpg
   ```

   La requête est automatiquement réacheminée et l’utilisateur voit cet objet :

   ```
   https://amzn-s3-demo-bucket.s3.amazonaws.com/images/image.jpg
   ```

   Pour acheminer les requêtes vers votre CloudFront distribution plutôt que vers votre compartiment Amazon S3, vous devez utiliser la méthode fournie par votre fournisseur de services DNS pour mettre à jour l'enregistrement de ressources CNAME défini pour votre domaine. Cet enregistrement CNAME mis à jour redirige les requêtes DNS de votre domaine vers le nom de CloudFront domaine de votre distribution. Pour plus d’informations, consultez la documentation fournie par votre prestataire de services DNS.

   > **Note**
   >
   > Si vous utilisez Route 53 comme service DNS, vous pouvez utiliser un jeu d’enregistrements de ressources d’alias ou CNAME. Pour plus d’informations sur la modification des jeux d’enregistrements de ressources, consultez Modification des enregistrements. Pour plus d’informations sur les jeux d’enregistrements de ressources

d’alias, consultez Choix entre des enregistrements avec ou sans alias. Les deux rubriques se trouvent dans le Guide du développeur Amazon Route 53.

Pour plus d'informations sur l'utilisation de CNames avec CloudFront, consultezthe section called “Utilisation d’URL personnalisées”.

Après avoir mis à jour le jeu d’enregistrements de ressources CNAME, un délai maximum de 72 heures peut être nécessaire pour que la modification se propage dans tout le système DNS, mais cela se produit en général plus vite. Pendant ce temps, certaines demandes concernant votre contenu continueront d'être acheminées vers votre compartiment Amazon S3, tandis que d'autres le seront. CloudFront

Déplacer un compartiment Amazon S3 vers un autre Région AWS

Si vous utilisez Amazon S3 comme origine pour une CloudFront distribution et que vous déplacez le compartiment vers une autre distribution Région AWS, la mise à jour de ses enregistrements afin d'utiliser la nouvelle région CloudFront peut prendre jusqu'à une heure lorsque les deux conditions suivantes sont remplies :

- Vous utilisez une identité CloudFront d'accès d'origine (OAI) pour restreindre l'accès au compartiment.
- vous déplacez le compartiment vers une région Amazon S3 qui exige Signature version 4 pour l’authentification.

Lorsque vous utilisez OAI, CloudFront utilise la région (entre autres valeurs) pour calculer la signature utilisée pour demander des objets à votre compartiment. Pour en savoir plus sur les OAI, consultez the section called “Utilisation d’une identité d’accès d’origine (héritée, non recommandée)”. Pour une liste de ceux Régions AWS qui prennent en charge la version 2 de Signature, voir le processus de signature de la version 2 de Signature dans le Référence générale d'Amazon Web Services.

Pour forcer une mise à jour plus rapide CloudFront des enregistrements, vous pouvez mettre à jour votre CloudFront distribution, par exemple en mettant à jour le champ Description dans l'onglet Général de la CloudFront console. Lorsque vous mettez à jour une distribution, vérifie CloudFront immédiatement la région dans laquelle se trouve votre compartiment. La propagation du changement à tous les emplacements périphériques ne doit prendre que quelques minutes.

Utiliser un point d' Multi-Region accès Amazon S3

Vous pouvez également utiliser un point d' Multi-Region accès Amazon S3 comme CloudFront origine. Les points Multi-Region d'accès Amazon S3 fournissent un point de terminaison global qui achemine automatiquement les demandes vers le compartiment Amazon S3 le plus proche en fonction de la latence du réseau. Lorsque vous utilisez un point d' Multi-Region accès Amazon S3 comme origine, spécifiez le nom d'hôte du point d' Multi-Region accès comme nom de domaine d'origine :

```
multi-region-access-point-alias.accesspoint.s3-global.amazonaws.com
```

Pour restreindre l'accès au point Multi-Region d'accès S3 afin qu'il ne soit accessible que par le biais de votre CloudFront distribution, consultezthe section called “Restreindre l'accès à l'origine d'un point Multi-Region d'accès Amazon S3”.

Utiliser un MediaStore conteneur ou un MediaPackage canal

Pour diffuser des vidéos en streaming CloudFront, vous pouvez configurer un compartiment Amazon S3 configuré en tant que MediaStore conteneur, ou créer un canal et des points de terminaison avec MediaPackage. Ensuite, vous créez et configurez une distribution CloudFront pour diffuser la vidéo.

Pour plus d’informations et pour obtenir des instructions détaillées, consultez les rubriques suivantes :

- the section called “Diffusez une vidéo en utilisant AWS Elemental MediaStore comme origine”
- the section called “Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage”

Utilisation d’un Application Load Balancer

Vous pouvez l'utiliser CloudFront pour acheminer le trafic vers des équilibreurs de charge d'application internes et accessibles à Internet.

Si votre origine consiste en un ou plusieurs serveurs HTTP(S) (serveurs web) hébergés sur une ou plusieurs instances Amazon EC2, vous pouvez choisir un Application Load Balancer accessible sur Internet pour distribuer le trafic vers les instances. Un équilibreur de charge accessible sur Internet possède un nom DNS publiquement résolu et achemine les demandes des clients vers les cibles via Internet.

Pour plus d'informations sur l'utilisation d'un Application Load Balancer connecté à Internet comme point de départ, notamment sur la manière de s'assurer que CloudFront les utilisateurs ne peuvent

accéder à vos serveurs Web que par le CloudFront biais de l'équilibreur de charge et non en accédant directement à l'équilibreur de charge, consultez. the section called “Restriction de l’accès aux Application Load Balancers”

Vous pouvez également utiliser les origines VPC pour diffuser du contenu à partir d’applications hébergées par un Application Load Balancer interne dans les sous-réseaux privés de votre cloud privé virtuel (VPC). Les origines VPC empêchent tout accès à votre application depuis l’internet public. Pour plus d’informations, consultez Restriction de l’accès avec les origines de VPC.

Utilisation d’un Network Load Balancer

Vous pouvez utiliser des équilibreurs de charge réseau internes et connectés à Internet avec Amazon. CloudFront Vous pouvez utiliser des équilibreurs de charge réseau internes dans des sous-réseaux privés CloudFront en utilisant des origines VPC. CloudFront Les origines VPC vous permettent de diffuser du contenu provenant d'applications hébergées dans des sous-réseaux VPC privés sans les exposer à l'Internet public. Pour plus d’informations, consultez Restriction de l’accès avec les origines de VPC.

Vous pouvez également l'utiliser CloudFront pour acheminer du trafic à partir d'équilibreurs de charge réseau connectés à Internet. Un équilibreur de charge connecté à Internet possède un nom DNS pouvant être résolu publiquement et peut recevoir des demandes provenant à la fois de clients sur Internet et de distributions. CloudFront

Utilisation d’une URL de fonction Lambda

Une URL de fonction Lambda est un point de terminaison HTTPS dédié à une fonction Lambda. Vous pouvez utiliser une URL de fonction Lambda pour créer une application web sans serveur entièrement dans Lambda. Vous pouvez appeler l'application Web Lambda directement via l'URL de fonction, sans avoir besoin de l'intégrer à API Gateway ou à un Application Load Balancer.

Si vous créez une application Web sans serveur en utilisant des fonctions Lambda avec des URL de fonction, vous pouvez en CloudFront ajouter pour bénéficier des avantages suivants :

- Accélérer votre application en mettant en cache le contenu plus près des utilisateurs
- Utiliser un nom de domaine personnalisé pour votre application Web
- Acheminez différents chemins d'URL vers différentes fonctions Lambda à l'aide CloudFront de comportements de cache
- Bloquer des demandes spécifiques en utilisant des restrictions CloudFront géographiques ou AWS WAF (ou les deux)

- AWS WAF À utiliser CloudFront pour protéger votre application contre les robots malveillants, empêcher les exploits courants des applications et améliorer la protection contre les attaques DDoS

Pour utiliser l'URL d'une fonction Lambda comme origine d'une CloudFront distribution, spécifiez le nom de domaine complet de l'URL de la fonction Lambda comme domaine d'origine. Un nom de domaine d'URL de fonction Lambda utilise le format suivant :

function-URL-ID.lambda-url.*AWS-Region*.on.aws

Lorsque vous utilisez l'URL d'une fonction Lambda comme origine d'une CloudFront distribution, l'URL de la fonction doit être accessible au public. Pour ce faire, utilisez l'une des options suivantes :

- Si vous utilisez le contrôle d'accès à l'origine (OAC), le `AuthType` paramètre de l'URL de la fonction Lambda doit utiliser `AWS_IAM` la valeur et autoriser les autorisations `lambda:InvokeFunction` et dans une `lambda:InvokeFunctionUrl` politique basée sur les ressources. Pour plus d'informations sur l'utilisation des URL de fonction Lambda pour l'OAC, consultez Restreindre l'accès à un AWS Lambda origine de l'URL de la fonction.
- Si vous n'utilisez pas l'OAC, vous pouvez définir le paramètre `AuthType` de l'URL de fonction sur `NONE` et autoriser l'autorisation `lambda:InvokeFunctionUrl` dans une stratégie basée sur les ressources.

Vous pouvez également ajouter un en-tête d'origine personnalisé aux demandes CloudFront envoyées à l'origine et écrire un code de fonction pour renvoyer une réponse d'erreur si l'en-tête n'est pas présent dans la demande. Cela permet de s'assurer que les utilisateurs ne peuvent accéder à votre application Web que par le biais de l'URL de la fonction Lambda CloudFront, et non directement à l'aide de celle-ci.

Pour plus d'informations sur les URL de fonction Lambda, consultez les rubriques suivantes dans le Guide du développeur AWS Lambda :

- URL de fonctions Lambda : présentation de la fonctionnalité d'URL de fonction Lambda
- Appel d'URL de fonctions Lambda : inclut des détails sur les charges utiles de demande et de réponse à utiliser pour coder votre application Web sans serveur
- Modèle de sécurité et d'authentification pour les URL de fonctions Lambda : inclut des détails sur les types d'authentification Lambda

Utilisez un AWS Lambda Fonction Web

Une fonction Web Lambda est une application Web qui s'exécute sur son propre point de terminaison HTTPS AWS Lambda et fournit celui-ci. Le point de terminaison peut être régional, qui dessert la fonction Web Lambda depuis une seule région Région AWS, ou global, qui la dessert depuis plusieurs régions. Vous pouvez utiliser une fonction Web Lambda comme origine d'une CloudFront distribution.

Si vous diffusez une application Web à partir d'une fonction Web Lambda, vous pouvez en ajouter CloudFront pour bénéficier des avantages suivants :

- Accélérez votre application en mettant en cache les réponses au plus près des utilisateurs, ce qui réduit également la charge de votre fonction Web Lambda
- Utilisez un nom de domaine personnalisé et votre propre certificat TLS pour votre application Web
- Acheminez différents chemins d'URL vers différentes fonctions Web Lambda ou d'autres origines en utilisant CloudFront des comportements de cache
- Bloquer des demandes spécifiques en utilisant des restrictions CloudFront géographiques ou AWS WAF (ou les deux)
- AWS WAF À utiliser CloudFront pour protéger votre application contre les robots malveillants, empêcher les exploits courants des applications et améliorer la protection contre les attaques DDoS
- Utilisez le contrôle d'accès à l'origine (OAC) pour vous assurer que les utilisateurs peuvent accéder à votre fonction Web Lambda uniquement via CloudFront

Pour utiliser une fonction Web Lambda comme origine d'une CloudFront distribution, spécifiez le nom d'hôte de son point de terminaison comme domaine d'origine. CloudFront identifie le type de point de terminaison à partir du nom d'hôte :

- Point de terminaison régional (`HomeRegion`et types de `PerRegion` points de terminaison) : le nom d'hôte se termine par `.lambda-web.`*`AWS-Region`*`.on.aws`
- Point de terminaison global (type de `MultiRegion` point de terminaison) : le nom d'hôte se termine par `.lambda-web.global.on.aws`

Pour utiliser le contrôle d'accès à l'origine (OAC) avec une fonction Web Lambda, le type d'authentification du point de terminaison doit être. `IamAuth` La politique basée sur les ressources de la fonction Web Lambda doit également autoriser l'autorisation.

`lambda:InvokeWebFunctionEndpoint` CloudFront signe les demandes aux points de terminaison régionaux avec Sigv4 et aux points de terminaison globaux avec Sigv4a. Pour plus d'informations, consultez Restreindre l'accès à un AWS Lambda Origine de la fonction Web.

Pour plus d'informations sur les fonctions Web Lambda, consultez les rubriques suivantes du guide du AWS Lambda développeur :

- AWS Lambda Fonctions Web — Présentation générale de la fonctionnalité Lambda Web Functions
- Points de terminaison des fonctions Web Lambda : inclut des détails sur les types de points de terminaison régionaux et mondiaux et leurs noms d'hôte
- Contrôle d'accès aux terminaux : inclut des détails sur les types d'authentification des points de terminaison et sur la manière dont les CloudFront demandes sont signées

Utilisation d'Amazon EC2 (ou autre origine personnalisée)

Vous pouvez utiliser des instances EC2 internes et connectées à Internet avec Amazon. CloudFront Vous pouvez utiliser des instances EC2 internes dans des sous-réseaux privés CloudFront en utilisant les origines VPC. CloudFront Les origines VPC vous permettent de diffuser du contenu provenant d'applications hébergées dans des sous-réseaux VPC privés sans les exposer à l'Internet public. Pour plus d'informations, consultez Restriction de l'accès avec les origines de VPC.

Une origine personnalisée est un serveur web HTTP(S) dont le nom DNS est publiquement résolu et qui achemine les demandes des clients vers des cibles via Internet. Le serveur HTTP (S) peut être hébergé sur une instance Amazon EC2, par AWS exemple, ou ailleurs. Une origine Amazon S3 configurée comme point de terminaison d'un site web est également considérée comme une origine personnalisée. Pour plus d'informations, consultez the section called "Utilisation d'un compartiment Amazon S3 configuré en tant que point de terminaison de site web".

Lorsque vous utilisez votre propre serveur HTTP comme origine personnalisée, vous spécifiez le nom DNS du serveur, ainsi que les ports HTTP et HTTPS et le protocole que vous souhaitez utiliser CloudFront pour récupérer des objets depuis votre origine.

La plupart des CloudFront fonctionnalités sont prises en charge lorsque vous utilisez une origine personnalisée, à l'exception du contenu privé. Bien que vous puissiez utiliser une URL signée pour distribuer du contenu à partir d'une origine personnalisée, CloudFront pour accéder à l'origine personnalisée, celle-ci doit rester accessible au public. Pour plus d'informations, consultez the section called "Restriction de contenu avec des URL et des cookies signés".

Suivez ces instructions pour utiliser des instances Amazon EC2 et d'autres origines personnalisées avec. CloudFront

- Hébergez et servez le même contenu sur tous les serveurs qui diffusent du contenu pour la même origine CloudFront. Pour plus d'informations, consultez the section called "Paramètres d'origine" dans la rubrique the section called "Tous les paramètres de distribution".
- Enregistrez les entrées `X-Amz-Cf-Id` d'en-tête sur tous les serveurs au cas où vous en auriez besoin Support ou CloudFront pour utiliser cette valeur pour le débogage.
- Limitez-les demandes d'accès aux ports HTTP et HTTPS sur lesquels votre origine personnalisée écoute.
- Synchronisez les horloges de tous les serveurs de votre implémentation. Notez que le temps universel coordonné (UTC) est CloudFront utilisé pour les URL signées et les cookies signés, pour les journaux et les rapports. En outre, si vous surveillez CloudFront l'activité à l'aide de CloudWatch métriques, notez que l'UTC est CloudWatch également utilisé.
- Utilisez des serveurs redondants pour gérer les défaillances.
- Pour plus d'informations sur l'utilisation d'une origine personnalisée pour servir un contenu privé consultez the section called "Restriction de l'accès à des fichiers d'origines personnalisées".
- Pour plus d'informations sur le comportement de demande et de réponse, ainsi que sur les codes d'état HTTP pris en charge, consultez Comportement des demandes et des réponses.

Si vous utilisez Amazon EC2 pour une origine personnalisée, nous vous recommandons de procéder comme suit :

- Utilisez un Amazon Machine Image qui installe automatiquement le logiciel d'un serveur web. Pour de plus amples informations, consultez la documentation Amazon EC2.
- Utilisez un équilibreur de charge Elastic Load Balancing pour gérer le trafic entre plusieurs instances Amazon EC2 et isoler votre application des modifications apportées aux instances Amazon EC2. Par exemple, si vous utilisez un équilibreur de charge, vous pouvez ajouter et supprimer les instances Amazon EC2 sans modifier votre application. Pour plus d'informations, consultez la documentation relative à Elastic Load Balancing.
- Lorsque vous créez votre CloudFront distribution, spécifiez l'URL de l'équilibreur de charge pour le nom de domaine de votre serveur d'origine. Pour plus d'informations, consultez the section called "Créer une distribution".

Utiliser des groupes CloudFront d'origine

Vous pouvez spécifier un groupe d'origine pour votre CloudFront origine si, par exemple, vous souhaitez configurer le basculement d'origine pour les scénarios nécessitant une haute disponibilité. Utilisez le basculement d'origine pour désigner une origine principale et une CloudFront deuxième origine qui passe CloudFront automatiquement à une origine lorsque l'origine principale renvoie des réponses d'échec spécifiques au code d'état HTTP.

Pour plus d’informations, notamment les étapes de configuration d’un groupe d’origine, consultez the section called “Augmentation de la disponibilité avec le basculement d’origine”.

Utilisation d’Amazon API Gateway

Vous pouvez utiliser API Gateway comme origine personnalisée pour votre CloudFront distribution. Pour plus d’informations, consultez les rubriques suivantes :

- Sécurisation d'Amazon API Gateway avec des chiffrements sécurisés à l'aide d'un article de blog Amazon CloudFront AWS
- Comment configurer API Gateway avec ma propre CloudFront distribution ? AWS re:Post

Activer IPv6 pour les CloudFront distributions

Amazon CloudFront prend en charge les protocoles IPv4 et IPv6, des clients aux sites AWS périphériques. CloudFront prend également en charge la connectivité IPv6 et double pile (IPv4 et IPv6) vers les origines. Vous obtenez ainsi une distribution IPv6 de bout en bout.

IPv6 est le protocole Internet de nouvelle génération conçu pour remplacer IPv4. L’IPv4 repose sur des adresses de 32 bits (comme 192.0.2.44), tandis que l’IPv6 repose sur des adresses de 128 bits (comme 2001:0db8:85a3::8a2e:0370:7334). L’IPv6 offre un espace d’adressage étendu afin d’accueillir un plus grand nombre d’appareils connectés à Internet.

Rubriques

- Demandes utilisateur en IPv6
- Demandes d’origine en IPv6

Demandes utilisateur en IPv6

En règle générale, vous devez activer IPv6 si certains de vos utilisateurs sur les réseaux IPv6 souhaitent accéder à vos contenus. Toutefois, n'activez pas le protocole IPv6 si les deux conditions suivantes sont remplies :

- Vous utilisez des URL signées ou des cookies signés pour restreindre l'accès à votre contenu.
- Vous utilisez une politique personnalisée qui inclut le `IpAddress` paramètre permettant de restreindre les adresses IP autorisées à accéder à votre contenu.

Si vous souhaitez limiter l’accès à un contenu spécifique par adresse IP et ne pas limiter l’accès aux autres contenus (ou limiter l’accès, mais pas par adresse IP), vous pouvez créer deux distributions. Pour plus d’informations sur la création d’URL signées à l’aide d’une politique personnalisée, consultez Création d’une URL signée utilisant une politique personnalisée. Pour plus d’informations sur la création de cookies signés à l’aide d’une politique personnalisée, consultez Définition de cookies signés utilisant une politique personnalisée.

Si vous utilisez un jeu d'enregistrements de ressources d'alias Route 53 pour acheminer le trafic vers votre CloudFront distribution, vous devez créer un deuxième ensemble d'enregistrements de ressources d'alias lorsque les deux conditions suivantes sont remplies :

- Vous activez IPv6 pour la distribution
- Vous utilisez d’autres noms de domaine dans les URL de vos objets

Pour plus d'informations, consultez la section Acheminer le trafic vers une CloudFront distribution Amazon en utilisant votre nom de domaine dans le guide du développeur Amazon Route 53.

Si vous avez créé un jeu d’enregistrements de ressources CNAME, que ce soit avec Route 53 ou avec un autre service DNS, vous n’avez besoin d’effectuer aucune modification. Un enregistrement CNAME achemine le trafic vers votre distribution, quel que soit le format d’adresse IP de la requête de visionneuse.

Si vous activez IPv6 et les journaux d' CloudFront accès, la `c-ip` colonne inclut des valeurs au format IPv4 et IPv6. Pour plus d’informations, consultez Champs du fichier journal.

> **Note**
>
> Pour maintenir une haute disponibilité des clients, CloudFront répondez aux demandes des utilisateurs en utilisant l'IPv4 si nos données suggèrent qu'IPv4 offrira une meilleure expérience utilisateur. Pour connaître le pourcentage de demandes traitées via CloudFront IPv6, activez la CloudFront journalisation de votre distribution et analysez la `c-ip` colonne, qui contient l'adresse IP de l'utilisateur à l'origine de la demande. Ce pourcentage augmentera dans le temps, mais il restera minoritaire car IPv6 n'est pas encore pris en charge par tous les réseaux du monde des utilisateurs. Certains réseaux d'utilisateur offrent une excellente prise en charge d'IPv6, tandis que d'autres ne prennent pas du tout en charge IPv6. (Un réseau de visionneuse est similaire à votre opérateur sans fil ou Internet).
> Pour plus d'informations sur notre prise en charge d'IPv6, consultez FAQ CloudFront . Pour en savoir plus sur l'activation des journaux d'accès, consultez les champs Journalisation standard et Préfixe de journal.

Demandes d'origine en IPv6

Lorsque vous utilisez une origine personnalisée (à l'exception d'Amazon S3), vous pouvez personnaliser les paramètres d'origine pour votre distribution. Ces paramètres vous permettent de choisir le mode de CloudFront connexion à votre point d'origine à l'aide d'adresses IPv4 ou IPv6. Pour les origines personnalisées (à l'exception d'Amazon S3), vous disposez des options de connectivité suivantes :

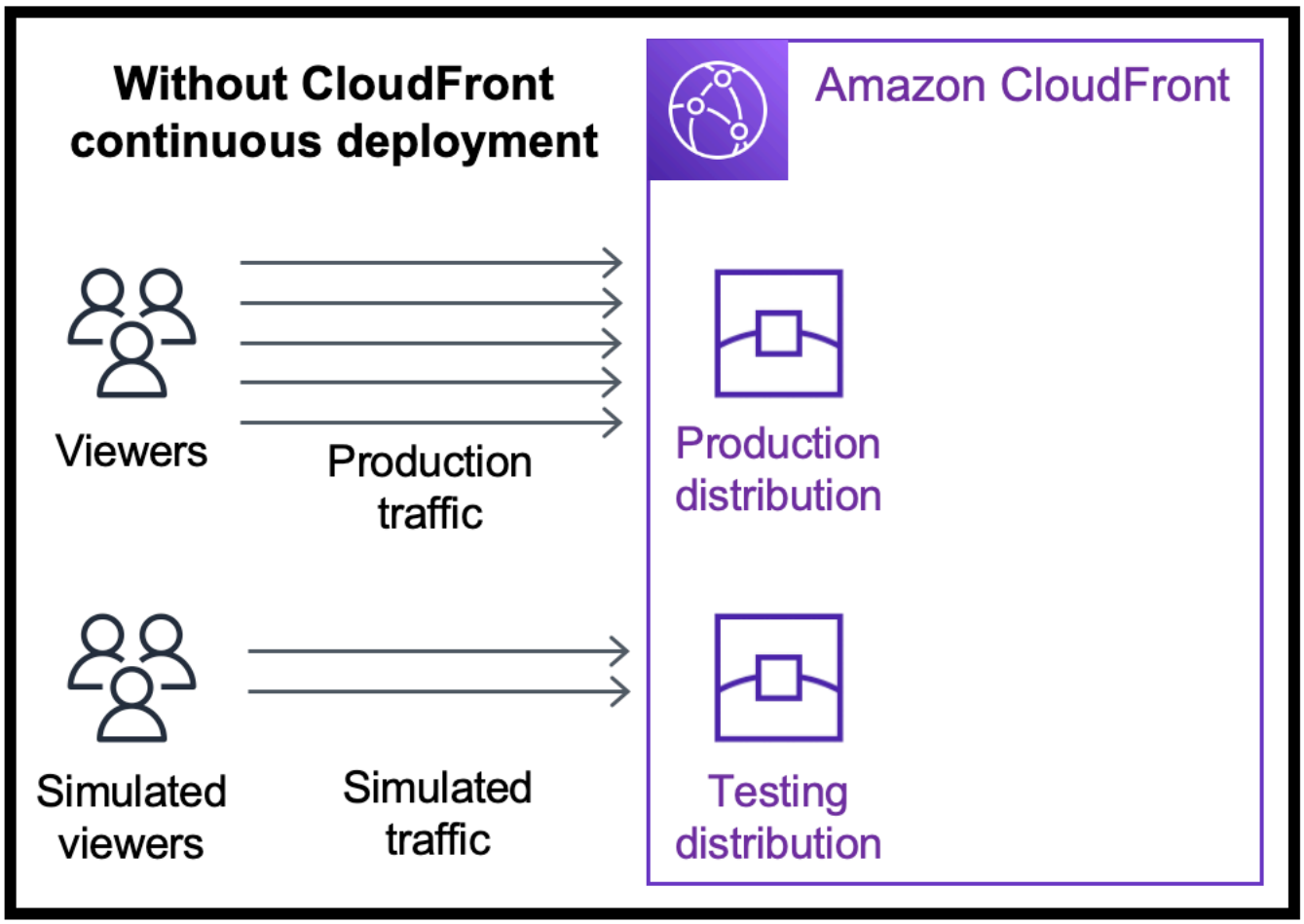
- IPv4 uniquement (par défaut) : il s'agit de la configuration par défaut CloudFront utilisée pour se connecter aux origines via IPv4.
- IPv6 uniquement (à l'exception des origines Amazon S3 et VPC) : nécessite que votre domaine d'origine soit converti en adresse IPv6. CloudFront utilise exclusivement des adresses IPv6 pour les connexions d'origine.
- Dual-stack— Active les connexions via IPv4 et IPv6. CloudFront choisit automatiquement la connectivité d'origine IPv4 ou IPv6 pour prioriser les performances et la disponibilité afin que vous puissiez l'utiliser CloudFront comme passerelle Internet à double pile IPv6 et IPv4 pour vos applications Web.

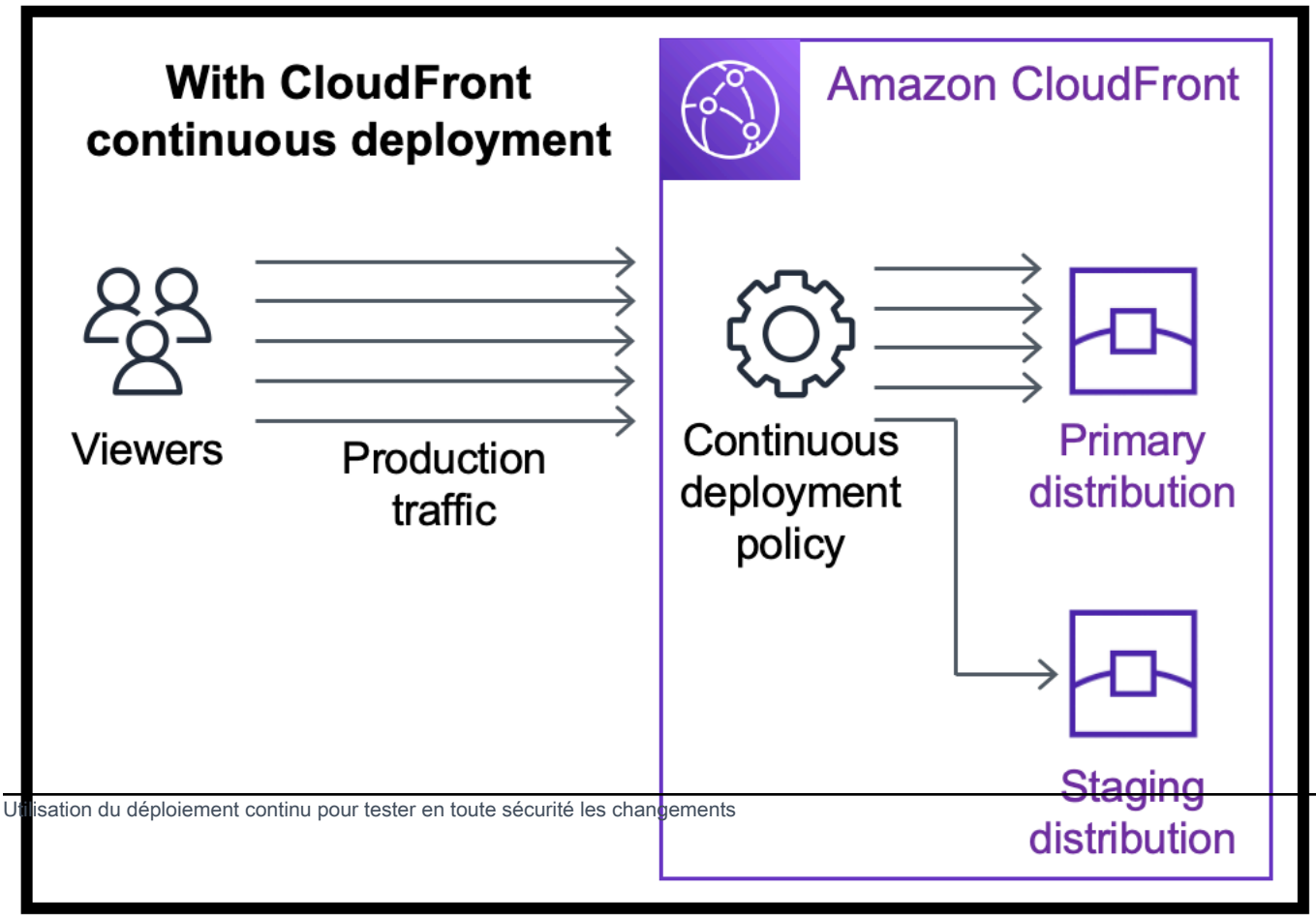
Choisissez l’option qui correspond à la configuration réseau et aux exigences de connectivité de votre origine. Pour plus d’informations, consultez Conception du DNS pour l’IPv6 et Considérations de sécurité et de surveillance pour l’IPv6.

Utilisez le déploiement CloudFront continu pour tester en toute sécurité les modifications de configuration du CDN

Avec le déploiement CloudFront continu d'Amazon, vous pouvez déployer en toute sécurité les modifications apportées à votre configuration CDN en effectuant d'abord des tests avec un sous-ensemble du trafic de production. Vous pouvez utiliser une distribution intermédiaire et une politique de déploiement continu pour envoyer une partie du trafic provenant d’utilisateurs réels (de production) vers la nouvelle configuration du CDN et vérifier qu'elle fonctionne comme prévu. Vous pouvez surveiller les performances de la nouvelle configuration en temps réel et promouvoir la nouvelle configuration pour qu'elle couvre l'ensemble du trafic en utilisant la distribution principale lorsque vous êtes prêt.

Le schéma suivant montre les avantages du déploiement CloudFront continu. Sans cela, vous devriez tester les changements de configuration du CDN sur un trafic simulé. Avec le déploiement continu, vous pouvez tester les changements sur un sous-ensemble du trafic de production, puis promouvoir les changements vers la distribution principale lorsque vous êtes prêt.


Without CloudFront continuous deployment
Amazon CloudFront
Viewers
Production traffic
Production distribution
Simulated viewers
Simulated traffic
Testing distribution


With CloudFront continuous deployment
Amazon CloudFront
Viewers
Production traffic
Continuous deployment policy
Primary distribution
Staging distribution

Pour en savoir plus sur l'utilisation du déploiement continu, consultez les rubriques suivantes.

Rubriques

- CloudFront flux de travail de déploiement continu
- Utilisation d'une distribution intermédiaire et d'une politique de déploiement continu
- Surveillance d'une distribution intermédiaire
- Découvrez le fonctionnement du déploiement continu
- Quotas et autres considérations relatives au déploiement continu

CloudFront flux de travail de déploiement continu

Le flux de travail de haut niveau suivant explique comment tester et déployer en toute sécurité des modifications de configuration dans le cadre d' CloudFront un déploiement continu.

1. Choisissez la distribution que vous souhaitez utiliser comme distribution principale. La distribution principale sert actuellement le trafic de production.
2. À partir de la distribution principale, créez une distribution intermédiaire. Une distribution intermédiaire commence comme une copie de la distribution principale.
3. Créez une configuration de trafic dans une politique de déploiement continu et associez-la à la distribution principale. Cela détermine la manière dont le trafic est CloudFront acheminé vers la distribution intermédiaire. Pour plus d'informations sur l'acheminement des demandes vers une distribution intermédiaire, consultez the section called "Routage des demandes vers la distribution intermédiaire".
4. Mettez à jour la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called "Mise à jour des distributions principale et intermédiaire".
5. Surveillez la distribution intermédiaire pour déterminer si les changements de configuration fonctionnent comme prévu. Pour plus d'informations sur la surveillance d'une distribution intermédiaire, consultez the section called "Surveillance d'une distribution intermédiaire".

   Lorsque vous surveillez la distribution intermédiaire, vous pouvez :

   - Remettre à jour la configuration de la distribution intermédiaire pour continuer à tester les changements de configuration.
   - Mettre à jour la politique de déploiement continu (configuration du trafic) pour envoyer plus ou moins de trafic vers la distribution intermédiaire.

6. Lorsque vous êtes satisfait des performances de la distribution intermédiaire, promouvez la configuration de la distribution intermédiaire vers la distribution principale. La configuration de la distribution intermédiaire est ainsi copiée vers la distribution principale. Cela désactive également la politique de déploiement continu, ce qui signifie que tout le trafic est CloudFront acheminé vers la distribution principale.

Vous pouvez créer une automatisation qui surveille les performances de la distribution intermédiaire (étape 5) et promeut automatiquement la configuration (étape 6) lorsque certains critères sont remplis.

Après avoir promu une configuration, vous pouvez réutiliser la même distribution intermédiaire la prochaine fois que vous souhaitez tester un changement de configuration.

Pour plus d'informations sur l'utilisation des distributions intermédiaires et des politiques de déploiement continu dans la CloudFront console AWS CLI, l'API ou l' CloudFront API, consultez la section suivante.

Utilisation d’une distribution intermédiaire et d’une politique de déploiement continu

Vous pouvez créer, mettre à jour et modifier des distributions intermédiaires et des politiques de déploiement continu dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Création d’une distribution intermédiaire avec une politique de déploiement continu

Les procédures suivantes expliquent comment créer une distribution intermédiaire avec une politique de déploiement continu.

Console

Vous pouvez créer une distribution intermédiaire avec une politique de déploiement continu à l’aide de la Console de gestion AWS.

Pour créer une distribution intermédiaire et une politique de déploiement continu (console)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.

3. Choisissez la distribution que vous souhaitez utiliser comme distribution principale. La distribution principale sert actuellement le trafic de production, c'est celle à partir de laquelle vous allez créer la distribution intermédiaire.
4. Dans la section Continuous deployment (Déploiement continu), choisissez Create staging distribution (Créer une distribution intermédiaire). L'assistant Create staging distribution (Créer une distribution intermédiaire) s'ouvre.
5. Dans l'assistant Create staging distribution (Créer une distribution intermédiaire), procédez comme suit :

   a. (Facultatif) Saisissez une description pour la distribution intermédiaire.

   b. Choisissez Next (Suivant).

   c. Modifiez la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called “Mise à jour des distributions principale et intermédiaire”.

      Lorsque vous avez terminé de modifier la configuration de la distribution intermédiaire, choisissez Next (Suivant).

   d. Utilisez la console pour spécifier la configuration du trafic. Cela détermine la manière dont le trafic est CloudFront acheminé vers la distribution intermédiaire. (CloudFront stocke la configuration du trafic dans une politique de déploiement continu.)

      Pour plus d'informations sur les options d'une configuration de trafic, consultez the section called “Routage des demandes vers la distribution intermédiaire”.

      Lorsque vous avez terminé la configuration du trafic, choisissez Next (Suivant).

   e. Passez en revue la configuration de la distribution intermédiaire, y compris la configuration du trafic, puis choisissez Create staging distribution (Créer une distribution intermédiaire).

Lorsque vous avez terminé l'assistant de création d'une distribution intermédiaire dans la CloudFront console CloudFront , procédez comme suit :

- Crée une distribution intermédiaire avec les paramètres que vous avez spécifiés (à l'étape 5c)
- Crée une politique de déploiement continu avec la configuration du trafic que vous avez spécifiée (à l'étape 5d)

- Attache la politique de déploiement continu à la distribution principale à partir de laquelle vous avez créé la distribution intermédiaire

Lorsque la configuration de la distribution principale, avec la politique de déploiement continu attachée, est déployée vers des emplacements périphériques, CloudFront commence à envoyer la partie spécifiée du trafic à la distribution intermédiaire en fonction de la configuration du trafic.

CLI

Pour créer une distribution intermédiaire et une politique de déploiement continu avec le AWS CLI, utilisez les procédures suivantes.

Pour créer une distribution intermédiaire (interface de ligne de commande)

1. Utilisez les commandes aws cloudfront get-distribution et grep ensemble pour obtenir la valeur `ETag` de la distribution que vous souhaitez utiliser comme distribution principale. La distribution principale sert actuellement le trafic de production, c'est celle à partir de laquelle vous allez créer la distribution intermédiaire.

   Voici un exemple de commande. Dans l'exemple suivant, remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.

   ```
   aws cloudfront get-distribution --id primary_distribution_ID | grep 'ETag'
   ```

   Copiez la valeur `ETag` car vous en aurez besoin à l'étape suivante.
2. Utilisez la commande aws cloudfront copy-distribution pour créer une distribution intermédiaire. L'exemple de commande suivant utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande. Dans l'exemple de commande suivant :

   - Remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.
   - Remplacez *`primary_distribution_ETag`* par la `ETag` valeur de la distribution principale (que vous avez obtenue à l'étape précédente).
   - (Facultatif) *`CLI_example`* Remplacez-le par le numéro de référence de l'appelant souhaité.

```
aws cloudfront copy-distribution --primary-distribution-
id primary_distribution_ID \
                                 --if-match primary_distribution_ETag \
                                 --staging \
                                 --caller-reference 'CLI_example'
```

La sortie de la commande affiche des informations sur la distribution intermédiaire et sa configuration. Copiez le nom de CloudFront domaine de la distribution intermédiaire, car vous en aurez besoin pour l'étape suivante.

Pour créer une politique de déploiement continu (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `continuous-deployment-policy.yaml` qui contient tous les paramètres d'entrée de la commande create-continuous-deployment-policy. La commande suivante utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande.

```
aws cloudfront create-continuous-deployment-policy --generate-cli-skeleton yaml-
input \
                                                    > continuous-deployment-
policy.yaml
```

2. Ouvrez le fichier nommé `continuous-deployment-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de la politique de déploiement continu de votre choix, puis enregistrez le fichier. Lorsque vous modifiez le fichier :

   - Dans la section `StagingDistributionDnsNames` :
     - Remplacez la valeur de `Quantity` par 1.
     - Pour cela`Items`, collez le nom de CloudFront domaine de la distribution intermédiaire (que vous avez enregistré lors d'une étape précédente).
   - Dans la section `TrafficConfig` :
     - Choisissez un `Type`, `SingleWeight` ou `SingleHeader`.
     - Supprimez les paramètres de l'autre type. Par exemple, si vous souhaitez une configuration du trafic basée sur le poids, définissez `Type` sur `SingleWeight`, puis supprimez les paramètres de `SingleHeaderConfig`.

- Pour utiliser une configuration de trafic basée sur le poids, définissez la valeur de `Weight` sur un nombre décimal compris entre `.01` (un pour cent) et `.15` (quinze pour cent).

Pour plus d'informations sur les options de `TrafficConfig`, consultez the section called "Routage des demandes vers la distribution intermédiaire" et the section called "Permanence des sessions pour les configurations basées sur le poids".

3. Utilisez la commande suivante pour créer la politique de déploiement continu à l'aide des paramètres d'entrée du fichier `continuous-deployment-policy.yaml`.

```
aws cloudfront create-continuous-deployment-policy --cli-input-yaml file://
continuous-deployment-policy.yaml
```

Copiez la valeur `Id` dans la sortie de la commande. Il s'agit de l'ID de la politique de déploiement continu, dont vous aurez besoin lors d'une étape suivante.

Pour attacher une politique de déploiement continu à une distribution principale (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de la distribution principale dans un fichier nommé `primary-distribution.yaml`. Remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.

```
aws cloudfront get-distribution-config --id primary_distribution_ID --output
 yaml > primary-distribution.yaml
```

2. Ouvrez le fichier nommé `primary-distribution.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

- Collez l'ID de la politique de déploiement continu (que vous avez copié lors d'une étape précédente) dans le champ `ContinuousDeploymentPolicyId`.
- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution principale afin d'utiliser la politique de déploiement continu. Remplacez *primary_distribution_ID* par l'ID de la distribution principale.

```
aws cloudfront update-distribution --id primary_distribution_ID --cli-input-yaml
 file://primary-distribution.yaml
```

Lorsque la configuration de la distribution principale, avec la politique de déploiement continu attachée, est déployée vers des emplacements périphériques, CloudFront commence à envoyer la partie spécifiée du trafic à la distribution intermédiaire en fonction de la configuration du trafic.

API

Pour créer une politique de distribution intermédiaire et de déploiement continu avec l' CloudFront API, utilisez les opérations d'API suivantes :

- CopyDistribution
- CreateContinuousDeploymentPolicy

Pour plus d'informations sur les champs que vous spécifiez dans ces appels d'API, consultez :

- the section called “Routage des demandes vers la distribution intermédiaire”
- the section called “Permanence des sessions pour les configurations basées sur le poids”
- La documentation de référence de l'API pour votre AWS SDK ou autre client d'API

Après avoir créé une distribution intermédiaire et une politique de déploiement continu, utilisez UpdateDistribution(sur la distribution principale) pour associer la stratégie de déploiement continu à la distribution principale.

Mise à jour d’une distribution intermédiaire

Les procédures suivantes expliquent comment mettre à jour une distribution intermédiaire avec une politique de déploiement continu.

Console

Vous pouvez mettre à jour certaines configurations pour la distribution principale et la distribution intermédiaire. Pour plus d'informations, consultez Mise à jour des distributions principale et intermédiaire.

Pour mettre à jour une distribution intermédiaire (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez la distribution principale. Il s'agit de la distribution qui sert actuellement le trafic de production, celle à partir de laquelle vous avez créé la distribution intermédiaire.
4. Choisissez View staging distribution (Afficher la distribution intermédiaire).
5. Utilisez la console pour modifier la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called "Mise à jour des distributions principale et intermédiaire".

Dès que la configuration de la distribution intermédiaire est déployée vers des emplacements périphériques, elle prend effet pour le trafic entrant acheminé vers la distribution intermédiaire.

CLI

Pour mettre à jour une distribution intermédiaire (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de la distribution intermédiaire dans un fichier nommé `staging-distribution.yaml`. Remplacez *`staging_distribution_ID`* par l'ID de la distribution intermédiaire.

```
aws cloudfront get-distribution-config --id staging_distribution_ID --output
 yaml > staging-distribution.yaml
```

2. Ouvrez le fichier nommé `staging-distribution.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

- Modifiez la configuration de la distribution intermédiaire. Pour plus d'informations sur les paramètres que vous pouvez mettre à jour, consultez the section called “Mise à jour des distributions principale et intermédiaire”.
- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la configuration de la distribution intermédiaire. Remplacez *`staging_distribution_ID`* par l'ID de la distribution intermédiaire.

```
aws cloudfront update-distribution --id staging_distribution_ID --cli-input-yaml
 file://staging-distribution.yaml
```

Dès que la configuration de la distribution intermédiaire est déployée vers des emplacements périphériques, elle prend effet pour le trafic entrant acheminé vers la distribution intermédiaire.

API

Pour mettre à jour la configuration d'une distribution intermédiaire, utilisez UpdateDistribution(sur la distribution intermédiaire) pour modifier la configuration de la distribution intermédiaire. Pour plus d’informations sur les paramètres que vous pouvez mettre à jour, consultez the section called “Mise à jour des distributions principale et intermédiaire”.

Mise à jour d’une politique de déploiement continu

Les procédures suivantes expliquent comment mettre à jour une politique de déploiement continu.

Console

Vous pouvez mettre à jour la configuration du trafic de votre distribution en mettant à jour la politique de déploiement continu.

Pour mettre à jour une politique de déploiement continu (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez la distribution principale. Il s'agit de la distribution qui sert actuellement le trafic de production, celle à partir de laquelle vous avez créé la distribution intermédiaire.
4. Dans la section Continuous deployment (Déploiement continu), choisissez Edit policy (Modifier la politique).
5. Modifiez la configuration du trafic dans la politique de déploiement continu. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

Lorsque la configuration de la distribution principale avec la politique de déploiement continu mise à jour est déployée sur des emplacements périphériques, CloudFront commence à envoyer du trafic vers la distribution intermédiaire en fonction de la configuration de trafic mise à jour.

CLI

Pour mettre à jour une politique de déploiement continu (interface de ligne de commande avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de la politique de déploiement continu dans un fichier nommé `continuous-deployment-policy.yaml`. Remplacez *`continuous_deployment_policy_ID`* par l'ID de la politique de déploiement continu. La commande suivante utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande.

```
aws cloudfront get-continuous-deployment-policy-config --
id continuous_deployment_policy_ID \
                                                    --output yaml >
 continuous-deployment-policy.yaml
```

2. Ouvrez le fichier nommé `continuous-deployment-policy.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Modifiez la configuration de la politique de déploiement continu comme vous le souhaitez. Par exemple, vous pouvez passer d'une configuration de trafic basée sur l'en-tête à une configuration de trafic basée sur le poids, ou vous pouvez modifier le pourcentage de trafic (poids) pour une configuration basée sur le poids. Pour plus d'informations, consultez the section called "Routage des demandes vers la distribution intermédiaire" et the section called "Permanence des sessions pour les configurations basées sur le poids".

- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la politique de déploiement continu. Remplacez *`continuous_deployment_policy_ID`* par l'ID de la politique de déploiement continu. La commande suivante utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande.

```
aws cloudfront update-continuous-deployment-policy --
id continuous_deployment_policy_ID \
                                                --cli-input-yaml file://
continuous-deployment-policy.yaml
```

Lorsque la configuration de la distribution principale avec la politique de déploiement continu mise à jour est déployée sur des emplacements périphériques, CloudFront commence à envoyer du trafic vers la distribution intermédiaire en fonction de la configuration de trafic mise à jour.

API

Pour mettre à jour une politique de déploiement continu, utilisez UpdateContinuousDeploymentPolicy.

Promouvoir la configuration d’une distribution intermédiaire

Les procédures suivantes expliquent comment promouvoir la configuration d’une distribution intermédiaire.

Console

Lorsque vous faites la promotion d'une distribution intermédiaire, CloudFront copie la configuration de la distribution intermédiaire vers la distribution principale. CloudFront désactive également la politique de déploiement continu et achemine tout le trafic vers la distribution principale.

Après avoir promu une configuration, vous pouvez réutiliser la même distribution intermédiaire la prochaine fois que vous souhaitez tester un changement de configuration.

Pour promouvoir la configuration d'une distribution intermédiaire (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez la distribution principale. Il s’agit de la distribution qui sert actuellement le trafic de production, celle à partir de laquelle vous avez créé la distribution intermédiaire.
4. Dans la section Continuous deployment (Déploiement continu), choisissez Promote (Promouvoir).
5. Saisissez **`confirm`**, puis choisissez Promote (Promouvoir).

CLI

Lorsque vous faites la promotion d'une distribution intermédiaire, CloudFront copie la configuration de la distribution intermédiaire vers la distribution principale. CloudFront désactive également la politique de déploiement continu et achemine tout le trafic vers la distribution principale.

Après avoir promu une configuration, vous pouvez réutiliser la même distribution intermédiaire la prochaine fois que vous souhaitez tester un changement de configuration.

Pour promouvoir la configuration d'une distribution intermédiaire (interface de ligne de commande)

- Utilisez la commande aws cloudfront update-distribution-with-staging-config pour promouvoir la configuration de la distribution intermédiaire vers la distribution principale. L'exemple de commande suivant utilise des caractères d'échappement (\) et des sauts de ligne pour plus de lisibilité, mais vous devez les omettre dans la commande. Dans l’exemple de commande suivant :
  - Remplacez *`primary_distribution_ID`* par l'ID de la distribution principale.
  - Remplacez *`staging_distribution_ID`* par l'ID de la distribution intermédiaire.
  - Remplacez *`primary_distribution_ETag`* et *`staging_distribution_ETag`* par les `ETag` valeurs des distributions principale et intermédiaire. Assurez-vous que la valeur de la distribution principale s’affiche en premier, comme indiqué dans l'exemple.

```
aws cloudfront update-distribution-with-staging-config --
id primary_distribution_ID \
                                                    --staging-distribution-
id staging_distribution_ID \
                                                    --if-match
 'primary_distribution_ETag,staging_distribution_ETag'
```

API

Pour promouvoir la configuration d'une distribution intermédiaire vers la distribution principale, utilisez UpdateDistributionWithStagingConfig.

Surveillance d’une distribution intermédiaire

Pour surveiller les performances d'une distribution intermédiaire, vous pouvez utiliser les mêmes mesures, journaux et rapports que ceux CloudFront fournis pour toutes les distributions. Par exemple :

- Vous pouvez consulter les mesures de CloudFront distribution par défaut (telles que le nombre total de demandes et le taux d'erreur) dans la CloudFront console, et vous pouvez activer des mesures supplémentaires (telles que le taux de réussite du cache et le taux d'erreur par code d'état) moyennant des frais supplémentaires. Vous pouvez également créer des alarmes en fonction de ces métriques.
- Vous pouvez consulter les journaux standard et les journaux d'accès en temps réel pour obtenir des informations détaillées sur les demandes reçues par la distribution intermédiaire. Les journaux standard contiennent les deux champs suivants qui vous aident à identifier la distribution principale à laquelle la demande a été initialement envoyée avant de l' CloudFront acheminer vers la distribution intermédiaire : `primary-distribution-id` et`primary-distribution-dns-name`.
- Vous pouvez consulter et télécharger des rapports dans la CloudFront console, par exemple le rapport sur les statistiques du cache.

Découvrez le fonctionnement du déploiement continu

Les rubriques suivantes expliquent le fonctionnement du déploiement CloudFront continu.

Rubriques

- Routage des demandes vers la distribution intermédiaire
- Permanence des sessions pour les configurations basées sur le poids
- Mise à jour des distributions principale et intermédiaire
- Les distributions principale et intermédiaire ne partagent pas de cache

Routage des demandes vers la distribution intermédiaire

Lorsque vous utilisez le déploiement CloudFront continu, il n'est pas nécessaire de modifier quoi que ce soit en ce qui concerne les demandes des utilisateurs. Les utilisateurs ne peuvent pas envoyer directement de demandes à une distribution intermédiaire à l'aide d'un nom DNS, d'une adresse IP ou d'un CNAME. Les utilisateurs envoient plutôt des demandes à la distribution principale (de production) et CloudFront acheminent certaines de ces demandes vers la distribution intermédiaire en fonction des paramètres de configuration du trafic définis dans la politique de déploiement continu. Il existe deux types de configurations du trafic :

Weight-based

Une configuration basée sur le poids achemine le pourcentage spécifié de demandes des utilisateurs vers la distribution intermédiaire. Lorsque vous utilisez une configuration basée sur le poids, vous pouvez également activer le maintien des sessions, ce qui permet de s'assurer que CloudFront les demandes provenant du même utilisateur sont traitées dans le cadre d'une seule session. Pour plus d’informations, consultez the section called “Permanence des sessions pour les configurations basées sur le poids”.

Header-based

Une configuration basée sur l’en-tête achemine les demandes vers la distribution intermédiaire lorsque la demande de l’utilisateur contient un en-tête HTTP spécifique (vous spécifiez l'en-tête et la valeur). Les demandes qui ne contiennent pas l'en-tête et la valeur spécifiés sont acheminées vers la distribution principale. Cette configuration est utile pour les tests locaux ou lorsque vous contrôlez les demandes des utilisateurs.

> **Note**
>
> Les en-têtes acheminés vers votre distribution intermédiaire doivent contenir le préfixe `aws-cf-cd-`.

Permanence des sessions pour les configurations basées sur le poids

Lorsque vous utilisez une configuration basée sur le poids pour acheminer le trafic vers une distribution intermédiaire, vous pouvez également activer la persistance des sessions, ce qui permet de garantir que CloudFront les demandes provenant du même visualiseur sont traitées comme une seule session. Lorsque vous activez le caractère permanent des sessions, CloudFront définit un cookie afin que toutes les demandes émanant d'un même utilisateur au cours d'une même session soient traitées par une seule distribution, principale ou intermédiaire.

Lorsque vous activez la permanence des sessions, vous pouvez également spécifier la durée d'inactivité. Si le visualiseur est inactif (n'envoie aucune demande) pendant cette durée, la session expire et CloudFront traite les futures demandes de ce visualiseur comme une nouvelle session. Vous spécifiez la durée d'inactivité en nombre de secondes, compris entre 300 (cinq minutes) et 3 600 (une heure).

Dans les cas suivants, CloudFront réinitialise toutes les sessions (même les sessions actives) et considère toutes les demandes comme une nouvelle session :

- Vous désactivez ou activez la politique de déploiement continu
- Vous désactivez ou activez le paramètre de permanence des sessions

Mise à jour des distributions principale et intermédiaire

Lorsqu'une une politique de déploiement continu est attachée à une distribution principale, les changements de configuration suivants sont disponibles pour les distributions principale et intermédiaire :

- Tous les paramètres de comportement du cache, y compris le comportement du cache par défaut
- Tous les paramètres d'origine (origines et groupes d'origines)
- Réponses d'erreur personnalisées (pages d'erreur)
- Restrictions géographiques
- Objet racine par défaut
- Paramètres de journalisation
- Description (commentaire)

Vous pouvez également mettre à jour les ressources externes référencées dans la configuration d'une distribution, telles qu'une politique de cache, une politique d'en-têtes de réponse, une CloudFront fonction ou une fonction Lambda @Edge.

Les distributions principale et intermédiaire ne partagent pas de cache

Les distributions principale et intermédiaire ne partagent pas de cache. Lorsque CloudFront la première demande est envoyée à une distribution intermédiaire, son cache est vide. Il commence à mettre en cache les réponses (s'il est configuré pour le faire) au fur et à mesure que les demandes atteignent la distribution intermédiaire.

Quotas et autres considérations relatives au déploiement continu

CloudFront le déploiement continu est soumis aux quotas suivants et à d'autres considérations.

Quotas

- Nombre maximum de distributions intermédiaires par Compte AWS : 20
- Nombre maximum de politiques de déploiement continu par Compte AWS : 20
- Pourcentage maximal de trafic que vous pouvez envoyer vers une distribution intermédiaire dans une configuration basée sur le poids : 15 %
- Valeurs minimale et maximale pour la durée d'inactivité de la permanence des sessions : 300 à 3 600 secondes

Pour plus d'informations, consultez Quotas.

> **Note**
>
> Lorsque vous utilisez le déploiement continu et que votre distribution principale est configurée avec une OAC pour l'accès au compartiment S3, mettez à jour votre stratégie de compartiment S3 afin d'autoriser l'accès pour la distribution intermédiaire. Pour consulter des exemples de stratégies de compartiment S3, reportez-vous à la the section called "Accorder l' CloudFront autorisation d'accéder au compartiment S3".

AWS WAF ACL Web

Si vous activez le déploiement continu pour votre distribution, les points suivants doivent être pris en compte pour AWS WAF :

- Vous ne pouvez pas associer de liste de contrôle d'accès AWS WAF Web (ACL) à la distribution si c'est la première fois que cette liste est associée à la distribution.
- Vous ne pouvez pas dissocier une ACL AWS WAF Web de la distribution.

Avant de pouvoir effectuer les tâches précédentes, vous devez supprimer la politique de déploiement continu pour votre distribution de production. Cette action supprime également la distribution intermédiaire. Pour plus d'informations, consultez Utilisation AWS WAF protections.

Cas où toutes les demandes sont CloudFront envoyées à la distribution principale

Dans certains cas, tels que les périodes de forte utilisation des ressources, toutes les demandes CloudFront peuvent être envoyées à la distribution principale, indépendamment de ce qui est spécifié dans la politique de déploiement continu.

CloudFront envoie toutes les demandes à la distribution principale pendant les heures de pointe, indépendamment de ce qui est spécifié dans la politique de déploiement continu. Le pic de trafic fait référence au trafic du CloudFront service, et non au trafic de votre distribution.

HTTP/3

Vous ne pouvez pas utiliser le déploiement continu avec une distribution compatible HTTP/3.

Utilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME)

Lorsque vous créez une distribution, CloudFront fournissez un nom de domaine pour celle-ci, tel que d111111abcdef8.cloudfront.net. Au lieu d'utiliser le nom de domaine fourni, vous pouvez utiliser un nom de domaine alternatif (également appelé CNAME).

Pour découvrir comment utiliser votre propre nom de domaine, par exemple, www.example.com, consultez les rubriques suivantes :

Rubriques

- Exigences relatives à l'utilisation de noms de domaines alternatifs
- Restrictions relatives à l'utilisation de noms de domaines alternatifs
- Ajout d'un nom de domaine alternatif
- Déplacement d'un nom de domaine alternatif
- Suppression d'un nom de domaine alternatif
- Utilisation des caractères génériques dans les noms de domaines alternatifs

Exigences relatives à l'utilisation de noms de domaines alternatifs

Lorsque vous ajoutez un autre nom de domaine, tel que www.example.com, à une CloudFront distribution, les conditions suivantes sont requises :

Les noms de domaines alternatifs doivent être en minuscules

Tous les noms de domaines alternatifs (CNAME) doivent être en minuscules.

Les noms de domaines alternatifs doivent être couverts par un certificat TLS valide

Pour ajouter un nom de domaine alternatif (CNAME) à une CloudFront distribution, vous devez joindre à votre distribution un certificat TLS valide et fiable qui couvre le nom de domaine alternatif. Cela garantit que seules les personnes ayant accès au certificat de votre domaine peuvent s'associer à CloudFront un CNAME lié à votre domaine.

Un certificat sécurisé est un certificat émis par AWS Certificate Manager (ACM) ou par une autre autorité de certification (CA) valide. Vous pouvez utiliser un certificat auto-signé pour valider un CNAME existant, mais pas pour un nouveau CNAME. CloudFront supporte les mêmes autorités de certification que Mozilla. Pour obtenir la liste actuelle, consultez Liste des certificats CA inclus dans Mozilla. Pour en savoir plus sur les certificats intermédiaires lors de l'utilisation d'une autorité de certification tierce, consultezCertificats intermédiaires.

Pour vérifier un autre nom de domaine à l'aide du certificat que vous joignez, y compris les noms de domaine alternatifs contenant des caractères génériques, CloudFront vérifiez le nom alternatif du sujet (SAN) sur le certificat. Le nom de domaine alternatif que vous ajoutez doit être couvert par le SAN.

> **Note**
>
> Un seul certificat peut être associé à une CloudFront distribution à la fois.

Vous prouvez que vous êtes autorisé à ajouter un nom de domaine alternatif spécifique à votre distribution en effectuant l'une des actions suivantes :

- Attacher un certificat qui inclut le nom de domaine alternatif, comme product-name.example.com.
- Attachement d'un certificat qui inclut un caractère générique * au début d'un nom de domaine, afin de couvrir plusieurs sous-domaines avec un même certificat. Lorsque vous spécifiez un caractère générique, vous pouvez ajouter plusieurs sous-domaines en tant que noms de domaines alternatifs dans CloudFront.

Les exemples suivants illustrent comment l'utilisation de caractères génériques dans les noms de domaines dans un certificat vous autorise à ajouter des noms de domaines alternatifs spécifiques dans CloudFront.

- Vous souhaitez ajouter marketing.example.com en tant que nom de domaine alternatif. Vous répertoriez dans votre certificat le nom de domaine suivant : *.example.com. Lorsque vous attachez ce certificat à CloudFront, vous pouvez ajouter n'importe quel autre nom de domaine pour votre distribution qui remplace le caractère générique à ce niveau, y compris marketing.example.com. Vous pouvez également, par exemple, ajouter les noms de domaines alternatifs suivants :
  - product.example.com
  - api.example.com

  Toutefois, vous ne pouvez pas ajouter des noms de domaines alternatifs qui sont à un niveau supérieur ou inférieur au caractère générique. Par exemple, vous ne pouvez pas ajouter les noms de domaines alternatifs example.com ou marketing.product.example.com.
- Vous souhaitez ajouter example.com en tant que nom de domaine alternatif. Pour ce faire, vous devez répertorier le nom de domaine example.com lui-même sur le certificat que vous attachez à votre distribution.
- Vous souhaitez ajouter marketing.product.example.com en tant que nom de domaine alternatif. Pour ce faire, vous pouvez répertorier *.product.example.com sur le certificat, ou répertorier marketing.product.example.com lui-même sur le certificat.

Autorisation de modifier la configuration DNS

Lorsque vous ajoutez des noms de domaine alternatifs, vous devez créer des enregistrements CNAME pour acheminer les requêtes DNS relatives aux noms de domaine alternatifs vers votre CloudFront distribution. Pour ce faire, vous devez être autorisé à créer des enregistrements CNAME auprès du fournisseur de services DNS pour les noms de domaines alternatifs que vous

utilisez. Cela signifie normalement que les domaines vous appartiennent, mais vous pouvez développer une application pour le propriétaire du domaine.

Noms de domaines alternatifs et HTTPS

Si vous souhaitez que les utilisateurs emploient HTTPS avec un nom de domaine alternatif, une configuration supplémentaire est nécessaire. Pour plus d'informations, consultez Utilisation de noms de domaines alternatifs et HTTPS.

Restrictions relatives à l'utilisation de noms de domaines alternatifs

Veuillez noter les restrictions suivantes relatives à l'utilisation de noms de domaines alternatifs :

Nombre maximum de noms de domaines alternatifs

Pour connaître le nombre maximum actuel de noms de domaine alternatifs que vous pouvez ajouter à une distribution ou demander un quota plus élevé (auparavant appelé limite), consultez Quotas généraux sur les distributions.

Duplication et chevauchement de noms de domaines alternatifs

Vous ne pouvez pas ajouter un autre nom de domaine à une CloudFront distribution si le même nom de domaine alternatif existe déjà dans une autre CloudFront distribution, même si l'autre distribution vous Compte AWS appartient.

Néanmoins, vous pouvez ajouter un nom de domaine alternatif à caractère générique, comme *.example.com, qui comporte (ou qui chevauche) un nom de domaine alternatif sans caractère générique, tel que www.example.com. Si vous avez des noms de domaine alternatifs qui se chevauchent dans deux distributions, CloudFront envoie la demande à la distribution dont le nom correspond le plus précisément, quelle que soit la distribution vers laquelle pointe l'enregistrement DNS. Par exemple, marketing.domain.com est plus spécifique que *. domain.com.

Si vous avez une entrée DNS générique pointant vers une CloudFront distribution et que vous recevez une erreur DNS mal configurée lorsque vous essayez d'ajouter un nouveau CNAME avec un nom plus spécifique, consultez. CloudFront renvoie une erreur d'enregistrement DNS mal configurée lorsque j'essaie d'ajouter un nouveau CNAME

Détournement de domaine

CloudFront offre une protection contre le fronting de domaine se produisant entre différents. Compte AWS Il s'agit d'un scénario dans lequel un client non standard crée une TLS/SSL

connexion à un nom de domaine dans un autre Compte AWS, puis fait une demande HTTPS pour un nom de domaine non lié dans un autre Compte AWS.

Par exemple, la connexion TLS peut se connecter à www.example.com, puis émettre une demande pour www.exemple.org.

Pour déterminer si une demande est transmise par un domaine, effectuez CloudFront les vérifications suivantes :

- L'extension SNI est identique à l'en-tête `Host` de la demande HTTP
- Le certificat appartient à la même distribution Compte AWS que celle de la demande
- L'`Host` de la demande HTTP est couvert par le certificat présenté lors de l'établissement d'une liaison TLS

Si aucune de ces conditions n'est remplie, CloudFront détermine que la demande est orientée vers le domaine. CloudFront rejettera la demande avec une réponse d'erreur HTTP 421.

> **Note**
>
> Si le client ne fournit pas l'extension SNI et obtient plutôt un certificat*.cloudfront.net par défaut, il CloudFront acceptera les demandes entrantes.

Comment CloudFront identifie la distribution d'une demande

CloudFront identifie une distribution pour une requête HTTP en fonction de l'`Host`en-tête. CloudFront ne dépend pas de l'adresse CloudFront IP à laquelle vous vous connectez ou de la poignée de main SNI fournie lors de la poignée de main TLS.

Lorsqu'il CloudFront reçoit une demande, il utilise la valeur de l'`Host`en-tête pour faire correspondre la demande à la distribution spécifique.

Supposons que vous disposiez de deux distributions et que vous ayez mis à jour votre configuration DNS afin que les noms de domaines alternatifs soient acheminés vers les points de terminaison suivants :

- primary.example.com pointe vers d111111primary.cloudfront.net
- secondary.example.com pointe vers d222222secondary.cloudfront.net

Si vous faites une demande https://primary.example.com mais que vous spécifiez l'`Host`en-tête comme secondary.example.com, par exemple`curl https://primary.example.com`

`-H "Host: secondary.example.com"`, la demande sera acheminée vers la distribution secondaire à la place.

Ajout d'un nom de domaine alternatif sur le nœud supérieur (zone apex) pour un domaine

Lorsque vous ajoutez un autre nom de domaine à une distribution, vous créez généralement un enregistrement CNAME dans votre configuration DNS pour acheminer les requêtes DNS relatives au nom de domaine vers votre CloudFront distribution. Cependant, il n'est pas possible de créer un enregistrement CNAME pour le nœud supérieur d'un espace de nom DNS, également appelé zone apex. Le protocole DNS ne le permet pas. Par exemple, si vous enregistrez le nom DNS example.com, la zone apex est example.com. Vous ne pouvez pas créer un enregistrement CNAME pour example.com, mais vous pouvez créer des enregistrements CNAME pour www.example.com, newproduct.example.com, etc.

Si vous utilisez Route 53 comme service DNS, vous pouvez créer un jeu d'enregistrements de ressources d'alias, qui présente les avantages suivants par rapport aux enregistrements CNAME :

- Vous pouvez créer un jeu d'enregistrements de ressources d'alias pour un nom de domaine sur le nœud supérieur (example.com).
- Vous pouvez créer un enregistrement HTTPS pour un nom de domaine alternatif afin de permettre la négociation du protocole dans le cadre de la recherche DNS si le client le prend en charge. Pour plus d'informations, consultez Create alias resource record set.
- Vous ne payez pas les requêtes Route 53 lorsque vous utilisez un jeu d'enregistrements de ressources d'alias.

> **Note**
>
> Si vous activez IPv6, vous devez créer deux jeux d'enregistrements de ressources d'alias : un pour acheminer le trafic IPv4 (un enregistrement A) et l'autre pour acheminer le trafic IPv6 (un enregistrement AAAA). Pour plus d'informations, consultez Activation d'IPv6 (demandes des utilisateurs) dans la rubrique Référence de tous les paramètres de distribution.

Pour plus d'informations, consultez la section Acheminer le trafic vers une distribution CloudFront Web Amazon en utilisant votre nom de domaine dans le guide du développeur Amazon Route 53.

Si vous n'utilisez pas Route 53 pour votre DNS, vous pouvez demander des adresses IP statiques Anycast pour acheminer des domaines apex tels que example.com vers. CloudFront Pour plus

d'informations, consultez Demande d'adresses IP statiques en unidiffusion à utiliser pour la liste d'autorisation.

Ajout d'un nom de domaine alternatif

La liste de tâches suivante décrit comment utiliser la CloudFront console pour ajouter un autre nom de domaine à votre distribution afin que vous puissiez utiliser votre propre nom de domaine dans vos liens au lieu du nom de CloudFront domaine. Pour plus d'informations sur la mise à jour de votre distribution à l'aide de l' CloudFront API, consultezConfiguration des distributions.

> **Note**
>
> Si vous souhaitez que les utilisateurs emploient HTTPS avec votre nom de domaine alternatif, consultez Utilisation de noms de domaines alternatifs et HTTPS.

Avant de commencer : Assurez-vous d'effectuer les opérations suivantes avant de mettre à jour votre distribution pour ajouter un nom de domaine alternatif :

- Enregistrez le nom de domaine auprès de Route 53 ou d'un autre registre de domaine.
- Obtenez un certificat TLS auprès d'une autorité de certification (CA) autorisée qui couvre le nom de domaine. Ajoutez le certificat à votre distribution pour vous assurer que vous êtes autorisé à utiliser le domaine. Pour plus d'informations, consultez Exigences relatives à l'utilisation de noms de domaines alternatifs.

Ajout d'un nom de domaine alternatif

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Dans l'onglet Général, choisissez Ajouter un domaine.
4. Entrez jusqu'à cinq domaines à desservir.
5. Choisissez Suivant.
6. Pour le certificat TLS, si vous ne CloudFront trouvez pas de certificat AWS Certificate Manager (ACM) existant pour votre domaine Compte AWS dans le `us-east-1` Région AWS, vous pouvez choisir de créer automatiquement un certificat ou de le créer manuellement dans ACM.

7. Une fois votre certificat approvisionné, vous devez mettre à jour vos enregistrements DNS auprès de votre fournisseur DNS afin de prouver la propriété du domaine. Les entrées que vous devez saisir dans vos enregistrements DNS vous sont fournies dans la CloudFront console.
8. Après avoir mis à jour vos enregistrements DNS, choisissez Valider le certificat.
9. Lorsque le certificat est validé, choisissez Suivant.
10. Passez en revue vos modifications et choisissez Ajouter des domaines.
11. Sous l'onglet Questions d'ordre général de la distribution, vérifiez que la valeur du champ Statut de distribution a été remplacée par Déployé. Si vous essayez d'utiliser un autre nom de domaine avant le déploiement des mises à jour de votre distribution, les liens que vous allez créer lors des étapes suivantes risquent de ne pas fonctionner.
12. Configurez le service DNS pour le nom de domaine alternatif (tel que www.example.com) afin d'acheminer le trafic vers le nom de CloudFront domaine de votre distribution (par exemple d111111abcdef8.cloudfront.net). La méthode utilisée varie selon que vous utilisiez ou non Route 53 comme fournisseur de services DNS pour le domaine. Pour plus d'informations, consultez Ajoutez un domaine à votre distribution CloudFront standard.

    Route 53

    Créez un jeu d'enregistrements de ressources d'alias. Avec un jeu d'enregistrements de ressources d'alias, vous ne payez pas pour les requêtes Route 53. Vous pouvez également créer un jeu d'enregistrements de ressources d'alias pour le nom de domaine racine (example.com), ce que DNS n'autorise pas pour les CNAME. Pour obtenir des instructions sur la création d'un ensemble d'enregistrements de ressources d'alias, consultez la section Router le trafic vers une distribution CloudFront Web Amazon en utilisant votre nom de domaine dans le guide du développeur Amazon Route 53.

    Vous pouvez éventuellement créer un enregistrement HTTPS pour un nom de domaine alternatif afin de permettre la négociation du protocole dans le cadre de la recherche DNS si le client le prend en charge.

    Pour créer un jeu d'enregistrements de ressources d'alias avec un enregistrement HTTPS (facultatif)

    1. Activez HTTP/2 ou HTTP/3 dans vos paramètres CloudFront de distribution. Pour plus d'informations, consultez Versions de HTTP prises en charge et Mettre à jour une distribution.

2. Dans la console Route 53, créez un jeu d'enregistrements de ressources d'alias. Suivez la procédure d'acheminement du trafic vers une distribution CloudFront Web Amazon en utilisant la procédure de votre nom de domaine.
3. Lorsque vous créez le jeu d'enregistrements de ressources d'alias, créez un enregistrement d'alias avec le type d'enregistrement HTTPS.

Autre fournisseur de services DNS

Utilisez la méthode fournie par votre fournisseur de services DNS pour ajouter un enregistrement CNAME à votre domaine. Ce nouvel enregistrement CNAME redirigera les requêtes DNS de votre nom de domaine alternatif (par exemple, www.exemple.com) vers le nom de CloudFront domaine de votre distribution (par exemple, d111111abcdef8.cloudfront.net). Pour plus d'informations, consultez la documentation fournie par votre prestataire de services DNS.

> **Important**
>
> Si vous possédez déjà un enregistrement CNAME pour votre autre nom de domaine, mettez-le à jour ou remplacez-le par un nouveau qui pointe vers le nom de CloudFront domaine de votre distribution.

13. Utilisez `dig` ou un outil DNS similaire pour vérifier que la configuration DNS créée à l'étape précédente pointe bien vers le nom de domaine de votre distribution.

L'exemple suivant illustre une requête `dig` sur le domaine images.example.com ainsi que la partie pertinente de la réponse.

```
PROMPT> dig www.example.com

; <<> DiG 9.3.3rc2 <<> www.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15917
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.     IN    A

;; ANSWER SECTION:
```

```
www.example.com. 10800 IN CNAME d111111abcdef8.cloudfront.net.
...
```

La section des réponses affiche un enregistrement CNAME qui achemine les requêtes pour www.example.com vers le nom de domaine de CloudFront distribution d111111abcdef8.cloudfront.net. Si le nom sur le côté droit de `CNAME` est le nom de domaine de votre CloudFront distribution, l'enregistrement CNAME est correctement configuré. Si cette valeur est différente (s'il s'agit, par exemple, du nom de domaine de votre compartiment Amazon S3), l'enregistrement CNAME n'est pas configuré correctement. Vous devez alors retourner à l'étape 7 et corriger l'enregistrement CNAME pour qu'il pointe vers le nom de domaine de votre distribution.

14. Testez le nom de domaine alternatif en visitant les URL avec votre nom de domaine au lieu du nom de domaine CloudFront de votre distribution.
15. Dans votre application, modifiez les URL de vos objets afin d'utiliser votre nom de domaine alternatif au lieu du nom de domaine de votre CloudFront distribution.

Déplacement d'un nom de domaine alternatif

Si vous essayez d'ajouter un nom de domaine alternatif à une distribution ou à un locataire de distribution standard et que ce nom de domaine alternatif est déjà associé à une autre ressource, vous recevrez un message d'erreur.

Ainsi, si vous tentez d'ajouter www.example.com à une distribution standard ou à un locataire de distribution et que ce nom de domaine alternatif est déjà associé à une autre ressource, CloudFront renverra l'erreur `CNAMEAlreadyExists` (Un ou plusieurs des CNAME que vous avez fournis sont déjà associés à une autre ressource).

Dans ce cas, vous pouvez déplacer le nom de domaine alternatif existant d'une ressource vers une autre. Il s'agit de la distribution source et de la distribution cible. Vous pouvez déplacer des noms de domaine alternatifs entre les locataires de distribution de l'une ou l'autre and/or des distributions standard.

Pour déplacer le nom de domaine alternatif, consultez les rubriques suivantes :

Rubriques

- Configuration de la distribution standard ou du locataire de distribution cibles
- Recherche de la distribution standard ou du locataire de distribution source

- Déplacer le nom de domaine alternatif

Configuration de la distribution standard ou du locataire de distribution cibles

Avant de déplacer un nom de domaine alternatif, vous devez configurer la ressource cible. Il s'agit de la distribution standard ou du locataire de distribution cible vers lequel vous déplacez le nom de domaine alternatif.

Standard distribution

Pour configurer une distribution standard cible

1. Demandez un certificat TLS. Ce certificat inclut le nom de domaine alternatif dans le champ Sujet ou dans le champ Domaine alternatif du sujet (SAN) ou bien un caractère générique (*) couvrant le nom de domaine alternatif que vous déplacez. Si vous n'en avez pas, vous pouvez en demander un auprès d' AWS Certificate Manager (ACM) ou d'une autre autorité de certification (CA), puis l'importer dans ACM.

   > **Note**
   >
   > Vous devez demander ou importer le certificat dans la région USA Est (Virginie du Nord) (`us-east-1`).

   Pour plus d'informations, consultez Demande de certificat public à partir de la console ou Importation d'un certificat dans AWS Certificate Manager dans le Guide de l'utilisateur AWS Certificate Manager .

2. Si vous n'avez pas encore créé la distribution standard cible, faites-le dès à présent. Lors de la création de la distribution standard, associez le certificat à cette distribution. Pour plus d'informations, consultez Créer une distribution.

   Si vous disposez déjà d'une distribution standard cible, associez le certificat à la distribution standard. Pour plus d'informations, consultez Mettre à jour une distribution.

3. Si vous déplacez des noms de domaine alternatifs au sein d'un même domaine Compte AWS, ignorez cette étape.

   Pour déplacer un autre nom de domaine de l'un Compte AWS à l'autre, vous devez créer un enregistrement TXT dans votre configuration DNS. Cette étape de vérification permet

d'empêcher les transferts de domaine non autorisés. CloudFront utilise cet enregistrement TXT pour valider que vous êtes propriétaire du nom de domaine alternatif.

Dans votre configuration DNS, créez un enregistrement TXT DNS qui associe le nom de domaine alternatif à la distribution standard cible. Le format d'enregistrement TXT peut varier en fonction du type de domaine.

- Pour les sous-domaines, ajoutez un trait de soulignement (_) devant le nom de domaine alternatif. Voici un exemple d'enregistrement TXT.

  ```
  _www.example.com TXT d111111abcdef8.cloudfront.net
  ```

- Pour un apex (ou un domaine racine), ajoutez un trait de soulignement et un point (_.) devant le nom de domaine. Voici un exemple d'enregistrement TXT.

  ```
  _.example.com TXT d111111abcdef8.cloudfront.net
  ```

Distribution tenant

Pour configurer le locataire de distribution cible

1. Demandez un certificat TLS. Ce certificat inclut le nom de domaine alternatif dans le champ Sujet ou dans le champ Domaine alternatif du sujet (SAN) ou bien un caractère générique (*) couvrant le nom de domaine alternatif que vous déplacez. Si vous n'en avez pas, vous pouvez en demander un auprès d' AWS Certificate Manager (ACM) ou d'une autre autorité de certification (CA), puis l'importer dans ACM.

   > **Note**
   >
   > Vous devez demander ou importer le certificat dans la région USA Est (Virginie du Nord) (`us-east-1`).

   Pour plus d'informations, consultez Demande de certificat public à partir de la console ou Importation d'un certificat dans AWS Certificate Manager dans le Guide de l'utilisateur AWS Certificate Manager .

2. Si vous n'avez pas encore créé le locataire de distribution cible, faites-le dès à présent. Lors de la création du locataire de distribution, associez le certificat à ce locataire. Pour plus d'informations, consultez Créer une distribution.

Si vous disposez déjà d'un locataire de distribution cible, associez le certificat à ce locataire de distribution. Pour plus d'informations, consultez Ajout d'un domaine et d'un certificat (locataire de distribution).

3. Si vous déplacez des noms de domaine alternatifs au sein d'un même domaine Compte AWS, ignorez cette étape.

   Pour déplacer un autre nom de domaine de l'un Compte AWS à l'autre, vous devez créer un enregistrement TXT dans votre configuration DNS. Cette étape de vérification permet d'empêcher les transferts de domaine non autorisés et CloudFront utilise cet enregistrement TXT pour valider que vous êtes bien le propriétaire du nom de domaine alternatif.

   Dans votre configuration DNS, créez un enregistrement TXT DNS qui associe le nom de domaine alternatif au locataire de distribution cible. Le format d'enregistrement TXT peut varier en fonction du type de domaine.

   - Pour les sous-domaines, ajoutez un trait de soulignement (_) devant le nom de domaine alternatif. Voici un exemple d'enregistrement TXT.

     ```
     _www.example.com TXT d111111abcdef8.cloudfront.net
     ```

   - Pour un apex (ou un domaine racine), ajoutez un trait de soulignement et un point (_.) devant le nom de domaine. Voici un exemple d'enregistrement TXT.

     ```
     _.example.com TXT d111111abcdef8.cloudfront.net
     ```

Consultez ensuite la rubrique suivante pour trouver la distribution standard ou le locataire de distribution source déjà associé(e) au nom de domaine alternatif.

Recherche de la distribution standard ou du locataire de distribution source

Avant de déplacer un nom de domaine alternatif d'une distribution (standard ou locataire) vers une autre, recherchez la distribution source. Il s'agit de la ressource à laquelle le nom de domaine alternatif est déjà associé. Lorsque vous connaissez l' Compte AWS ID des ressources de distribution source et cible, vous pouvez déterminer comment déplacer le nom de domaine secondaire.

> **Remarques**
>
> - Nous vous recommandons d'utiliser l'opération ListDomainConflictsAPI, car elle prend en charge à la fois les distributions standard et les locataires de distribution.

- Le fonctionnement de ListConflictingAliasesl'API ne prend en charge que les distributions standard.

Suivez ces exemples pour trouver la distribution source (standard ou locataire).

list-domain-conflicts

> **Tip**
>
> - Pour une distribution standard, vous devez disposer des autorisations `cloudfront:GetDistribution` et `cloudfront:ListDomainConflicts`.
> - Pour un locataire de distribution, vous devez disposer des autorisations `cloudfront:GetDistributionTenant` et `cloudfront:ListDomainConflicts`.

Pour utiliser **`list-domain-conflicts`** pour rechercher la distribution standard source ou le locataire de distribution

1. Utilisez la commande `list-domain-conflicts`, comme illustré dans l'exemple suivant.

   a. Remplacez *`www.example.com`* par le nom de domaine.

   b. Pour le `domain-control-validation-resource`, indiquez l'ID de la distribution standard cible ou du locataire de distribution cible que vous avez configuré précédemment. Vous devez disposer d'une distribution standard ou d'un locataire de distribution associé à un certificat couvrant le domaine spécifié.

   c. Exécutez cette commande en utilisant les informations d'identification identiques Compte AWS à celles de la distribution standard ou du locataire de distribution cible.

   Demande

   Cet exemple fait référence à un locataire de distribution.

```
aws cloudfront list-domain-conflicts \
--domain www.example.com \
--domain-control-validation-resource
 "DistributionTenantId=dt_2x9GhoK0TZRsohWzv1b9It8JABC"
```

Réponse

Pour chaque nom de domaine dans la sortie de la commande, les informations suivantes s'affichent :

- Le type de ressource auquel le domaine est associé
- L'ID de la ressource
- L' Compte AWS ID propriétaire de la ressource

L'ID de ressource et l'ID de compte sont partiellement masqués. Cette opération vous permet d'identifier la distribution standard ou le locataire de distribution relevant de votre compte, tout en protégeant les informations de ceux qui ne vous appartiennent pas.

```
{
    "DomainConflicts": [
        {
            "Domain": "www.example.com",
            "ResourceType": "distribution-tenant",
            "ResourceId": "***************ohWzv1b9It8JABC",
            "AccountId": "******112233"
        }
    ]
}
```

La réponse répertorie tous les noms de domaine qui sont en conflit ou qui se chevauchent avec celui que vous avez spécifié.

Exemple

- Si vous le spécifiez*tenant1.example.com*, la réponse inclut tenant1.example.com et le nom de domaine alternatif générique qui se chevauche (*.example.com s'il existe).
- Si vous le spécifiez**.tenant1.example.com*, la réponse inclut *.tenant1.example.com et tout autre nom de domaine couvert par ce caractère générique (par exemple, test.tenant1.example.com, dev.tenant1.example.com, etc.).

2. Dans la réponse, recherchez la distribution standard source ou le locataire de distribution pour le nom de domaine alternatif que vous souhaitez déplacer, et notez l' Compte AWS ID.

3. Comparez l'ID de compte de la distribution standard source ou du locataire de distribution source avec l'ID de compte dans lequel vous avez créé la distribution standard cible ou le locataire de distribution cible à l'étape précédente. Vous pouvez ensuite déterminer si la source et la cible se trouvent dans le même Compte AWS. Vous pouvez ainsi déterminer le mode de déplacement du nom de domaine alternatif.

   Pour plus d'informations, consultez la commande list-domain-conflicts dans la Référence de l'AWS Command Line Interface .

list-conflicting-aliases (standard distributions only)

> **Tip**
>
> Vous devez disposer des autorisations `cloudfront:GetDistribution` et `cloudfront:ListConflictingAliases` sur la distribution standard cible.

Pour utiliser des **`alias conflictuels de listes`** pour trouver la distribution standard source

1. Utilisez la commande `list-conflicting-aliases`, comme illustré dans l'exemple suivant.

   a. *`www.example.com`*Remplacez-le par le nom de domaine alternatif et *`EDFDVBD6EXAMPLE`* par l'ID de la distribution standard cible que vous avez configurée précédemment.

   b. Exécutez cette commande en utilisant les informations d'identification situées dans le même Compte AWS que la distribution standard.

   Demande

   Cet exemple fait référence à une distribution standard.

```
aws cloudfront list-conflicting-aliases \
--alias www.example.com \
--distribution-id EDFDVBD6EXAMPLE
```

   Réponse

Pour chaque nom de domaine alternatif dans la sortie de la commande, vous pouvez voir l'ID de la distribution standard à laquelle il est associé, ainsi que l'ID du Compte AWS propriétaire de cette distribution. Les ID de distribution standard et de compte sont partiellement masqués, ce qui vous permet d'identifier les distributions standard et les comptes que vous possédez, tout en protégeant les informations de ceux qui ne vous appartiennent pas.

```
{
    "ConflictingAliasesList": {
        "MaxItems": 100,
        "Quantity": 1,
        "Items": [
            {
                "Alias": "www.example.com",
                "DistributionId": "*******EXAMPLE",
                "AccountId": "******112233"
            }
        ]
    }
}
```

La réponse répertorie les noms de domaine alternatifs qui sont en conflit ou qui se chevauchent avec celui que vous avez spécifié.

Exemple

- Si vous le spécifiez*www.example.com*, la réponse inclut www.exemple.com et le nom de domaine alternatif générique qui se chevauche (*.exemple.com) s'il existe.
- Si vous le spécifiez**.example.com*, la réponse inclut *.example.com et tout autre nom de domaine couvert par ce caractère générique (par exemple, www.example.com, test.example.com, dev.example.com, etc.).

2. Recherchez la distribution standard pour le nom de domaine alternatif que vous souhaitez déplacer et notez son Compte AWS ID. Comparez cet ID de compte avec l'ID de compte sur lequel vous avez créé la distribution standard cible à l'étape précédente. Vous pouvez ensuite déterminer si ces deux distributions standard sont identiques Compte AWS et comment déplacer le nom de domaine alternatif.

   Pour plus d'informations, consultez la commande list-conflicting-aliases dans la Référence de l'AWS Command Line Interface .

Ensuite, consultez la rubrique suivante pour déplacer le nom de domaine alternatif.

Déplacer le nom de domaine alternatif

Selon le cas, choisissez parmi les méthodes suivantes pour déplacer le nom de domaine alternatif :

Les distributions source et cible (standard ou locataire) appartiennent au même Compte AWS

Utilisez la commande update-domain-association dans l' AWS Command Line Interface (AWS CLI) pour déplacer le nom de domaine alternatif.

Cette commande fonctionne pour tous les déplacements effectués au sein d'un même compte, y compris lorsque le nom de domaine alternatif est un domaine apex (également appelé domaine racine, comme exemple.com).

Les distributions source et cible (standard ou locataire) appartiennent à des Comptes AWS différents

Si vous avez accès à la distribution standard source ou au locataire de distribution, que le nom de domaine alternatif n'est pas un domaine apex et que vous n'utilisez pas de caractère générique qui chevauche ce nom de domaine alternatif, utilisez alors un caractère générique pour déplacer ce nom de domaine alternatif. Pour plus d'informations, consultez the section called "Utilisation d'un caractère générique pour déplacer un nom de domaine alternatif".

Si vous n'avez pas accès à la Compte AWS distribution standard source ou au tenant de distribution, vous pouvez essayer d'utiliser la update-domain-association commande pour déplacer le nom de domaine alternatif. La distribution standard source ou le locataire de distribution doit être désactivé avant de déplacer le nom de domaine alternatif. Pour obtenir de l'aide supplémentaire, consultez the section called "Contact AWS Support pour déplacer un autre nom de domaine".

> **Note**
>
> Vous pouvez utiliser la commande associate-alias, mais elle ne prend en charge que les distributions standard. Consultez AssociateAliasle manuel Amazon CloudFront API Reference.

update-domain-association (standard distributions and distribution tenants)

Pour utiliser **`update-domain-association`** pour déplacer un autre nom de domaine

1. Utilisez la commande `update-domain-association`, comme illustré dans l'exemple suivant.

   a. *`example.com`*Remplacez-le par le nom de domaine alternatif et spécifiez l'ID de la distribution standard ou du locataire de distribution cible.

   b. Exécutez cette commande en utilisant les informations d'identification situées dans le même Compte AWS que la distribution standard ou le locataire de distribution.

> Notez les restrictions suivants
>
> - En plus de l'autorisation `cloudfront:UpdateDomainAssociation`, vous devez disposer de l'autorisation `cloudfront:UpdateDistribution` pour mettre à jour une distribution standard. Pour mettre à jour un locataire de distribution, vous devez disposer de l'autorisation `cloudfront:UpdateDistributionTenant`.
> - Si les distributions source et cible (standard ou locataire) sont différentes Comptes AWS, la source doit être désactivée avant de pouvoir déplacer le domaine.
> - La distribution cible doit être configurée comme décrit dans the section called "Configuration de la distribution standard ou du locataire de distribution cibles".

Demande

```
aws cloudfront update-domain-association \
  --domain "www.example.com" \
  --target-resource DistributionTenantId=dt_9Fd3xTZq7Hl2KABC \
  --if-match E3UN6WX5ABC123
```

Réponse

```
{
    "ETag": "E7Xp1Y3N9DABC",
    "Domain": "www.example.com",
```

```
    "ResourceId": "dt_9Fd3xTZq7Hl2KABC"
}
```

Cette commande supprime le nom de domaine alternatif de la distribution standard source ou du locataire de distribution, puis l'ajoute à la distribution standard ou au locataire de distribution cibles.

2. Une fois la distribution cible entièrement déployée, mettez à jour votre configuration DNS pour faire pointer votre nom de domaine vers le point de terminaison CloudFront de routage. Par exemple, votre enregistrement DNS pointerait votre nom de domaine alternatif (`www.example.com`) vers le nom de domaine CloudFront fourni d111111abcdef8.cloudfront.net. Si la cible est un locataire de distribution, spécifiez le point de terminaison du groupe de connexions. Pour plus d'informations, consultez Pointer les domaines vers CloudFront.

associate-alias (standard distributions only)

Pour utiliser **`associate-alias`** pour déplacer un autre nom de domaine

1. Utilisez la commande `associate-alias`, comme illustré dans l'exemple suivant.

   a. *`www.example.com`*Remplacez-le par le nom de domaine alternatif et *`EDFDVBD6EXAMPLE`* par l'ID de distribution standard cible.

   b. Exécutez cette commande en utilisant les informations d'identification situées dans le même Compte AWS que la distribution standard.

   > Notez les restrictions suivants
   >
   > - Vous devez disposer des autorisations `cloudfront:AssociateAlias` et `cloudfront:UpdateDistribution` sur la distribution standard cible.
   > - Si la distribution standard source et cible se trouvent dans la même distribution Compte AWS, vous devez disposer d'une `cloudfront:UpdateDistribution` autorisation sur la distribution standard source.
   > - Si la distribution standard source et la distribution standard cible sont différentes Comptes AWS, vous devez d'abord désactiver la distribution standard source.

- La distribution standard cible doit être configurée comme décrit dans the section called “Configuration de la distribution standard ou du locataire de distribution cibles”.

Demande

```
aws cloudfront associate-alias \
--alias www.example.com \
--target-distribution-id EDFDVBD6EXAMPLE
```

Cette commande supprime le nom de domaine alternatif de la distribution standard source, puis l’ajoute à la distribution standard cible.

2. Une fois la distribution standard cible entièrement déployée, mettez à jour votre configuration DNS afin de pointer l’enregistrement DNS du nom de domaine alternatif vers le nom de domaine de distribution de la distribution standard cible. Par exemple, votre enregistrement DNS pointerait votre nom de domaine alternatif (`www.example.com`) vers le nom de domaine CloudFront fourni d111111abcdef8.cloudfront.net.

Pour plus d’informations, consultez la commande associate-alias dans la Référence des commandes de l’AWS CLI .

Utilisation d’un caractère générique pour déplacer un nom de domaine alternatif

Si la distribution source se trouve dans une distribution Compte AWS différente de la distribution cible et que la distribution source est activée, vous pouvez utiliser un caractère générique pour déplacer le nom de domaine secondaire.

> **Note**
>
> Vous pouvez utiliser un caractère générique pour déplacer un domaine apex (comme example.com). Pour déplacer un domaine apex lorsque les distributions source et cible se trouvent dans des Comptes AWS différents, contactez Support. Pour plus d’informations, consultez the section called “Contact AWS Support pour déplacer un autre nom de domaine”.

Pour utiliser un caractère générique pour déplacer un nom de domaine alternatif

> **Note**
>
> Ce processus implique plusieurs mises à jour de vos distributions. Attendez que chaque distribution déploie entièrement la dernière modification avant de passer à l'étape suivante.

1. Mettez à jour la distribution cible pour ajouter un nom de domaine alternatif couvrant le nom de domaine alternatif que vous déplacez. Si le nom de domaine alternatif que vous déplacez correspond à www.example.com, ajoutez le nom de domaine alternatif *.example.com à la distribution cible. Pour ce faire, le SSL/TLS certificat de la distribution cible doit inclure le nom de domaine générique. Pour plus d'informations, consultez the section called "Mettre à jour une distribution".
2. Mettez à jour les paramètres DNS du nom de domaine alternatif de manière à ce qu'il pointe vers le nom de domaine de la distribution cible. Par exemple, si le nom de domaine alternatif que vous déplacez correspond à www.example.com, mettez à jour l'enregistrement DNS correspondant à www.example.com de manière à acheminer le trafic vers le nom de domaine de la distribution cible (par exemple d111111abcdef8.cloudfront.net).

   > **Note**
   >
   > Même une fois les paramètres DNS mis à jour, le nom de domaine alternatif est toujours servi par la distribution source puisque c'est là que le nom de domaine alternatif est actuellement configuré.

3. Mettez à jour la distribution source pour supprimer le nom de domaine de remplacement. Pour plus d'informations, consultez Mettre à jour une distribution.
4. Mettez à jour la distribution cible pour ajouter le nom de domaine alternatif. Pour plus d'informations, consultez Mettre à jour une distribution.
5. Utilisez dig (ou un outil de requête DNS similaire) pour vérifier que l'enregistrement DNS du le nom de domaine alternatif est résolu avec le nom de domaine de la distribution cible.
6. (Facultatif) Mettez à jour la distribution cible pour supprimer le nom de domaine alternatif avec caractère générique.

Contact AWS Support pour déplacer un autre nom de domaine

Si les distributions source et cible sont différentes Comptes AWS et que vous n'avez pas accès à la distribution source Compte AWS ou que vous ne pouvez pas désactiver la distribution source, vous pouvez contacter Support pour déplacer le nom de domaine alternatif.

Pour contacter Support pour déplacer un autre nom de domaine

1. Configurez une distribution cible, y compris l'enregistrement TXT DNS qui pointe vers la distribution cible. Pour plus d'informations, consultez Configuration de la distribution standard ou du locataire de distribution cibles.
2. Contactez-nous Support pour leur demander de vérifier que vous êtes bien le propriétaire du domaine et de le déplacer vers la nouvelle CloudFront distribution pour vous.
3. Une fois la distribution cible entièrement déployée, mettez à jour votre configuration DNS afin de pointer l'enregistrement DNS du nom de domaine alternatif vers le nom de domaine de distribution de la distribution cible.

Suppression d'un nom de domaine alternatif

Si vous souhaitez arrêter le routage du trafic d'un domaine ou d'un sous-domaine vers une CloudFront distribution, suivez les étapes décrites dans cette section pour mettre à jour à la fois la configuration DNS et la CloudFront distribution.

Il est important que vous supprimiez les noms de domaine alternatifs de la distribution et que vous mettiez à jour votre configuration DNS. Cela permet d'éviter des problèmes ultérieurs si vous souhaitez associer le nom de domaine à une autre CloudFront distribution. Si un nom de domaine alternatif est déjà associé à une distribution, il ne peut pas être configuré avec une autre.

> **Note**
>
> Si vous souhaitez supprimer le nom de domaine alternatif de cette distribution afin de pouvoir l'ajouter à une autre, suivez les étapes indiquées dans Déplacement d'un nom de domaine alternatif. Si vous suivez plutôt les étapes décrites ici (pour supprimer un domaine) puis que vous ajoutez le domaine à une autre distribution, il y aura une période pendant laquelle le domaine ne sera pas lié à la nouvelle distribution car il CloudFront se propage aux mises à jour vers les emplacements périphériques.

Pour supprimer un autre nom de domaine d'une distribution

1. Pour commencer, acheminez le trafic Internet de votre domaine vers une autre ressource qui n'est pas votre CloudFront distribution, comme un équilibreur de charge Elastic Load Balancing. Vous pouvez également supprimer l'enregistrement DNS vers lequel le trafic est acheminé CloudFront.

   Effectuez l'une des opérations suivantes, en fonction du service DNS pour votre domaine :

   - Si vous utilisez Route 53, mettez à jour ou supprimez les enregistrements d'alias ou les enregistrements CNAME. Pour plus d'informations, consultez Modification des enregistrements ou Suppression des enregistrements.
   - Si vous utilisez un autre fournisseur de services DNS, utilisez la méthode fournie par ce fournisseur de services DNS pour mettre à jour ou supprimer l'enregistrement CNAME qui dirige le trafic vers CloudFront. Pour plus d'informations, consultez la documentation fournie par votre prestataire de services DNS.
2. Après avoir mis à jour les enregistrements DNS de votre domaine, attendez que les modifications se soient propagées et que les résolveurs DNS acheminent le trafic vers la nouvelle ressource. Vous pouvez vérifier si cette opération est terminée en créant des liens de test utilisant votre domaine dans l'URL.
3. Connectez-vous au Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home, puis mettez à jour votre CloudFront distribution pour supprimer le nom de domaine en procédant comme suit :

   a. Choisissez l'ID de la distribution que vous souhaitez mettre à jour.
   b. Sous l'onglet General, choisissez Edit.
   c. Dans Autres noms de domaine (CNAME), supprimez le nom de domaine alternatif (ou les noms de domaine) que vous ne souhaitez plus utiliser pour votre distribution.
   d. Choisissez Oui, Modifier.

Utilisation des caractères génériques dans les noms de domaines alternatifs

Lorsque vous ajoutez des noms de domaine alternatifs, vous pouvez utiliser le caractère générique * au début d'un nom de domaine au lieu d'ajouter individuellement les sous-domaines. Par exemple, avec comme nom de domaine alternatif *.example.com, vous pouvez par exemple utiliser n'importe quel nom de domaine qui se termine par example.com dans vos URL, comme www.example.com,

product-name.example.com, marketing.product-name.example.com, etc. Le chemin vers l'objet est identique, quel que soit le nom de domaine, par exemple :

- www.exemple. com/images/image.jpg
- nom du produit.exemple. com/images/image.jpg
- marketing.nom_produit.exemple. com/images/image.jpg

Suivez ces exigences pour les noms de domaine alternatifs qui incluent des caractères génériques :

- Le nom de domaine alternatif doit commencer par un astérisque et un point (*.).
- Vous ne pouvez pas utiliser un caractère générique pour remplacer une partie d'un nom de sous-domaine, comme cela : *domain.example.com.
- Vous ne pouvez pas remplacer un sous-domaine au milieu d'un nom de domaine, comme cela : subdomain.*.example.com.
- Tous les noms de domaines alternatifs, y compris les noms de domaines alternatifs qui utilisent des caractères génériques, doivent être couverts par le nom SAN (Subject Alternative Name) sur le certificat.

Un nom de domaine alternatif avec caractère générique, comme *.example.com, peut comporter un autre nom de domaine en cours d'utilisation, comme example.com.

Utilisation WebSockets avec les CloudFront distributions

Amazon CloudFront prend en charge l'utilisation WebSocket d'un TCP-based protocole utile lorsque vous avez besoin de connexions bidirectionnelles de longue durée entre les clients et les serveurs. Une connexion persistante est souvent une exigence avec des applications en temps réel. Les scénarios que vous pouvez utiliser WebSockets incluent les plateformes de chat social, les espaces de travail collaboratifs en ligne, les jeux multijoueurs et les services fournissant des flux de données en temps réel, tels que les plateformes de trading financier. Les données via une WebSocket connexion peuvent circuler dans les deux sens pour une communication en duplex intégral.

WebSocket la fonctionnalité est automatiquement activée pour fonctionner avec n'importe quelle distribution. Pour l'utiliserWebSockets, configurez l'une des options suivantes dans le comportement du cache associé à votre distribution :

- Transmettre tous les en-têtes de demande utilisateur à votre origine. Vous pouvez utiliser la politique de AllViewer gestion des demandes d'origine.
- Transférer spécifiquement les en-têtes de demande `Sec-WebSocket-Key` et `Sec-WebSocket-Version` dans votre politique de demande d'origine.

Comment fonctionne le WebSocket protocole

Le WebSocket protocole est un protocole indépendant qui vous permet d'éviter une partie de la surcharge (voire une latence accrue) du TCP-based protocole HTTP.

Pour établir une WebSocket connexion, le client envoie une requête HTTP normale qui utilise la sémantique de mise à niveau du protocole HTTP pour modifier le protocole. Le serveur peut ensuite terminer la liaison. La WebSocket connexion reste ouverte et le client ou le serveur peuvent s'envoyer des trames de données sans avoir à établir de nouvelles connexions à chaque fois.

Par défaut, le WebSocket protocole utilise le port 80 pour les WebSocket connexions régulières et le port 443 pour les WebSocket connexions via TLS. Les options que vous choisissez pour votre CloudFront Viewer Protocol Policy et que vous Protocole (origines personnalisées uniquement) appliquez aux WebSocket connexions ainsi qu'au trafic HTTP.

WebSocket exigences

WebSocket les demandes doivent être conformes à la RFC 6455 dans les formats standard suivants.

Example Exemple de demande du client

```
GET /chat HTTP/1.1
Host: server.example.com
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: dGhlIHNhbXBsZSBub25jZQ==
Origin: https://example.com
Sec-WebSocket-Protocol: chat, superchat
Sec-WebSocket-Version: 13
```

Example Exemple de réponse du serveur

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
```

```
Sec-WebSocket-Accept: s3pPLMBiTxaQ9kYGzzhZRbK+xOo=
Sec-WebSocket-Protocol: chat
```

Si la WebSocket connexion est déconnectée par le client ou le serveur, ou en raison d'une interruption du réseau, les applications clientes sont censées rétablir la connexion avec le serveur.

WebSocket En-têtes recommandés

Pour éviter des problèmes inattendus liés à la compression lors de l'utilisation WebSockets, nous vous recommandons d'inclure les en-têtes suivants dans une politique de demande d'origine :

- `Sec-WebSocket-Key`
- `Sec-WebSocket-Version`
- `Sec-WebSocket-Protocol`
- `Sec-WebSocket-Accept`
- `Sec-WebSocket-Extensions`

> **Note**
>
> Actuellement, CloudFront seules les WebSocket connexions via le HTTP/1.1 protocole sont prises en charge.

Demande d’adresses IP statiques en unidiffusion à utiliser pour la liste d’autorisation

Vous pouvez également utiliser votre propre plage d'adresses IP CloudFront au lieu des adresses IP statiques CloudFront-provided Anycast. Pour plus d’informations, consultez Utilisez votre propre adresse IP pour CloudFront utiliser IPAM.

Vous pouvez demander des adresses IP statiques à Anycast CloudFront pour les utiliser avec vos distributions. Les listes IP statiques Anycast ne peuvent contenir que des adresses IP IPv4 ou à la fois des adresses IP IPv4 et IPv6. Ces adresses IP vous sont dédiées Compte AWS et réparties dans différentes régions géographiques.

Vous pouvez demander l’ajout de 21 adresses IP statiques en unidiffusion à la liste d’autorisation auprès des fournisseurs réseau, afin de supprimer les frais de données pour les utilisateurs qui

accèdent à votre application. Vous pouvez également utiliser ces adresses IP statiques dans les pare-feux de sécurité sortants pour contrôler les échanges de trafic avec les applications approuvées. Les listes d'adresses IP statiques en unidiffusion peuvent être utilisées avec une ou plusieurs distributions.

Si vous souhaitez activer le routage des domaines apex (tels que exemple.com) directement vers vos CloudFront distributions, vous pouvez demander 3 adresses IP statiques Anycast pour ce cas d'utilisation. Ajoutez ensuite des enregistrements A dans votre DNS pour pointer le domaine apex vers CloudFront.

Les adresses IP statiques en unidiffusion fonctionnent avec Server Name Indication (SNI). Pour plus d'informations, consultez Utilisation d'une extension SNI pour traiter les demandes HTTPS (fonctionne pour la plupart des clients).

Conditions préalables

Pour utiliser les listes d'adresses IP statiques Anycast avec votre CloudFront distribution, vous devez sélectionner Utiliser tous les emplacements périphériques pour la classe de prix de la distribution. Pour plus d'informations sur la tarification, consultez Tarification d'CloudFront .

Demande d'une liste d'adresses IP statique en unidiffusion

Demandez une liste d'adresses IP statiques Anycast à utiliser avec votre CloudFront distribution.

Pour demander une liste d'adresses IP statique en unidiffusion

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, sélectionnez Adresses IP statiques.
3. Pour Request, cliquez sur le lien pour contacter l'ingénierie de CloudFront support.
4. Fournissez les informations relatives à votre charge de travail (octets de demande par seconde et demandes par seconde).
5. CloudFront l'ingénierie de support examine votre demande. Le processus de révision peut prendre jusqu'à deux jours.

Une fois votre demande approuvée, vous pouvez créer une liste d'adresses IP statiques en unidiffusion et l'associer à une ou plusieurs distributions.

Création d’une liste d’adresses IP statiques en unidiffusion

Avant de commencer, demandez une liste d’adresses IP statiques en unidiffusion comme expliqué dans la section précédente.

Pour créer une liste d’adresses IP statiques en unidiffusion

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, sélectionnez Adresses IP statiques.
3. Choisissez Créer une liste d’adresses IP en unidiffusion.
4. Pour Nom, entrez un nom.
5. Pour Cas d’utilisation d’une adresse IP statique, sélectionnez le cas d’utilisation approprié.
6. Pour le type d'adresse IP, spécifiez l'une des options suivantes :
   - IPv4 — Alloue une liste d'adresses IPv4 uniquement
   - Dualstack — Alloue une liste d'adresses IPv4 et IPv6
7. Consultez les conditions de service et la tarification, puis choisissez Envoyer.

Une fois votre liste d’adresses IP statiques créée, vous pouvez consulter les adresses IP allouées sur la page des détails de votre liste d’adresses IP statiques. Vous pouvez également associer des distributions à la liste d’adresses IP statiques.

Association d’une liste d’adresses IP statiques en unidiffusion à une distribution existante

Avant de commencer, demandez et créez une liste d’adresses IP statiques en unidiffusion comme expliqué dans les sections précédentes.

Vérifiez que les paramètres de distribution suivants sont compatibles avec votre liste d'adresses IP statiques Anycast :

- Catégorie de tarifspossède le paramètre Utiliser tous les emplacements périphériques (meilleures performances).
- Si IPv6 est activé, vous pouvez associer une liste d'adresses IP statiques Anycast à double pile. Une liste d'adresses IP statique Anycast contenant uniquement des adresses IPv4 ne peut pas être associée à des distributions où IPv6 est activé.

Pour associer une liste d'adresses IP statiques en unidiffusion à une distribution existante

- Effectuez l'une des actions suivantes :
  - Associez la liste d'adresses IP statiques depuis la page des détails de la liste d'adresses IP statiques :
    1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
    2. Dans le volet de navigation de gauche, sélectionnez Adresses IP statiques.
    3. Choisissez le nom de votre liste d'adresses IP statiques.
    4. Choisissez Association des distributions.
    5. Sélectionnez une ou plusieurs distributions, puis choisissez Association des distributions.
  - Associez la liste d'adresses IP statiques depuis la page des détails de la distribution :
    1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
    2. Dans le volet de navigation de gauche, choisissez Distributions.
    3. Choisissez le nom de votre distribution.
    4. Dans l'onglet Général, sous Paramètres, sélectionnez Modifier.
    5. Pour la Liste d'adresses IP en unidiffusion, sélectionnez la liste d'adresses IP statiques en unidiffusion à utiliser avec cette distribution.
    6. Cliquez sur Enregistrer les modifications.

Association d'une liste d'adresses IP statiques en unidiffusion à une nouvelle distribution

Avant de commencer, demandez et créez une liste d'adresses IP statiques en unidiffusion comme expliqué dans les sections précédentes.

Pour associer une liste d'adresses IP statiques en unidiffusion à une nouvelle distribution

- Créez une nouvelle distribution . Pour plus d'informations, consultez Création d'une CloudFront distribution dans la console. Dans Paramètres, vous devez choisir les options suivantes pour utiliser votre liste d'adresses IP statiques en unidiffusion :

- Pour Liste d’adresses IP en unidiffusion, sélectionnez votre liste d’adresses IP statiques en unidiffusion dans la liste déroulante.
- Pour Catégorie de tarifs sélectionnez Utiliser tous les emplacements périphériques (meilleure performance).
- Remarque : Si votre adresse IP statique Anycast utilise uniquement l'IPv4 et non le double stack, pour IPv6, sélectionnez Off.

Terminez la création de votre distribution. Vous pouvez choisir tous les autres paramètres et configurations qui ne sont pas nécessaires pour les listes d’adresses IP statiques en unidiffusion en fonction de vos besoins.

Pour plus d'informations sur les quotas liés aux listes d'adresses IP statiques Anycast, consultez la section CloudFront Points de terminaison et quotas Amazon dans le. Références générales AWS

Associer une liste IP statique Anycast à un groupe de connexion

Avant de commencer, demandez et créez une liste d'adresses IP statiques Anycast, comme expliqué dans les sections précédentes.

Pour associer une liste d'adresses IP statiques Anycast à un nouveau groupe de connexion

1. Assurez-vous d'avoir activé les groupes de connexion sous Paramètres.
2. Créez un groupe de connexion. Pour plus d'informations, consultez la section Créer un groupe de connexion personnalisé.
3. Pour les paramètres, vous devez effectuer les sélections suivantes pour utiliser votre liste d'adresses IP statiques Anycast.
   - Pour Liste d’adresses IP en unidiffusion, sélectionnez votre liste d’adresses IP statiques en unidiffusion dans la liste déroulante.
4. Terminez la création de votre groupe de connexion.

> **Note**
>
> Si votre adresse IP statique Anycast utilise uniquement l'IPv4 et non le double stack, pour IPv6, sélectionnez Off.

Pour plus d'informations sur les quotas liés aux listes d'adresses IP statiques Anycast, consultez la section CloudFront Points de terminaison et quotas Amazon dans le. Référence générale d'Amazon Web Services

Mettre à jour une liste d'adresses IP statiques Anycast

Après avoir créé votre adresse IP statique Anycast et l'avoir associée à une distribution, vous pouvez modifier le type d'adresse IP de votre liste d'adresses IP statiques Anycast.

Pour mettre à jour une liste d'adresses IP statiques Anycast

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, sélectionnez Adresses IP statiques.
3. Choisissez le nom de votre liste d’adresses IP statiques.
4. Choisissez Modifier.
5. Pour le type d'adresse IP, spécifiez l'une des options suivantes :

   - IPv4 — Alloue une liste d'adresses IPv4 uniquement
   - Dualstack — Alloue une liste d'adresses IPv4 et IPv6

   > **Note**
   >
   > Vous ne pouvez pas choisir IPv4 si votre distribution associée a déjà activé IPv6. Pour ce faire, désactivez IPv6 avant de mettre à jour le type d'adresse IP de votre adresse IP statique Anycast. Pour plus d’informations, consultez Activer IPv6 pour les CloudFront distributions.

6. Choisissez Soumettre pour enregistrer vos modifications et mettre à jour la liste d'adresses IP statiques d'Anycast.

Utilisez votre propre adresse IP pour CloudFront utiliser IPAM

Ce didacticiel montre comment utiliser IPAM pour gérer vos CIDR BYOIP pour les listes d'adresses IP statiques CloudFront Anycast.

Rubriques

- Qu'est-ce que le BYOIP pour les adresses IP statiques Anycast ?
- Pourquoi utiliser cette fonctionnalité ?
- Conditions préalables
- Étape 1 : demander une liste d'adresses IP statiques Anycast
- Étape 2 : Création d'une liste d'adresses IP statique Anycast
- Étape 3 : Création d'une CloudFront distribution
- Étape 4 : Associer aux CloudFront ressources
- Étape 5 : Préparation à la migration
- Étape 6 : Faites la promotion du CIDR dans le monde entier

Qu'est-ce que le BYOIP pour les adresses IP statiques Anycast ?

CloudFront permet d'apporter vos propres adresses IPv4 et IPv6 via le BYOIP d'IPAM pour les services mondiaux. Grâce à l'interface unifiée d'IPAM, les clients peuvent créer des pools d'adresses IP dédiés à l'aide de leurs propres adresses IP (BYOIP) et les attribuer à des CloudFront distributions tout en tirant parti du réseau AWS mondial de diffusion de contenu pour diffuser leurs applications et leurs contenus. Vos adresses IP sont annoncées à partir de plusieurs emplacements CloudFront périphériques simultanément à l'aide du routage anycast.

Pourquoi utiliser cette fonctionnalité ?

Contrôlez l'accès au réseau dans les listes d'autorisation pour :

- Allow-list Adresses IP auprès des fournisseurs de réseau pour éviter les frais de données pour les spectateurs approuvés
- Configurer les pare-feux de sécurité sortants pour limiter le trafic aux applications approuvées uniquement

Simplifier les opérations et les migrations

- Acheminez les domaines apex (exemple.com) directement vers CloudFront en ajoutant des enregistrements A qui pointent vers vos adresses IP statiques
- Migrez depuis d'autres CDN sans mettre à jour l'infrastructure IP ou les configurations de pare-feu
- Maintenir les listes d'autorisations de propriété intellectuelle existantes auprès des partenaires et des clients

- Partagez une seule liste d'adresses IP statiques Anycast entre plusieurs distributions CloudFront

Une image de marque cohérente

- Conservez votre espace d'adresse IP existant pour une image de marque cohérente lorsque vous passez à AWS

Conditions préalables

Pour utiliser les listes d'adresses IP statiques Anycast avec votre CloudFront distribution, vous devez sélectionner Utiliser tous les emplacements périphériques pour la classe de prix de la distribution. Pour plus d'informations sur la tarification, consultez Tarification d'CloudFront. Pour Bring Your Own IP (BYOIP), vous devez également désactiver IPv6 pour le groupe de distribution ou de connexion lorsque vous utilisez IPv4-only BYOIP. Pour le BYOIP à double pile, associez une liste d'adresses IP statiques Anycast à double pile et activez IPv6 pour le groupe de distribution ou de connexion.

Effectuez les étapes suivantes avant de commencer :

- Configuration IPAM : voir Intégrer l'IPAM aux comptes et Créer un IPAM.
- Vérification du domaine : vérifiez le contrôle du domaine.
- Créez un pool de niveau supérieur : suivez les étapes 1 à 2 de la section Apportez votre propre CIDR IPv4 à IPAM and/or .
- Créez un pool IPAM avec les paramètres régionaux comme globaux à CloudFront utiliser. Pour plus d'informations, voir Apporter votre propre adresse IP à CloudFront l'utilisation d'IPAM.

> **Note**
>
> Nécessite trois blocs d'adresse CIDR IPv4 and/or /24/48.

Étape 1 : demander une liste d'adresses IP statiques Anycast

Demandez une liste d'adresses IP statiques Anycast à utiliser avec votre CloudFront distribution.

Pour demander une liste d’adresses IP statique en unidiffusion

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, sélectionnez Adresses IP statiques.
3. Pour Request, cliquez sur le lien pour contacter l'ingénierie de CloudFront support.
4. Fournissez les informations relatives à votre charge de travail (octets de demande par seconde et demandes par seconde).
5. CloudFront l'ingénierie de support examine votre demande. Le processus de révision peut prendre jusqu’à deux jours.
6. Une fois votre demande approuvée, vous pouvez créer une liste d’adresses IP statiques en unidiffusion et l’associer à une ou plusieurs distributions.

Étape 2 : Création d'une liste d'adresses IP statique Anycast

Avant de commencer, demandez une liste d’adresses IP statiques en unidiffusion comme expliqué dans la section précédente.

Pour créer une liste d’adresses IP statiques en unidiffusion

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, sélectionnez Adresses IP statiques.
3. Choisissez Créer une liste d’adresses IP en unidiffusion.
4. Pour Nom, entrez un nom.
5. Pour les cas d'utilisation d'une adresse IP statique, sélectionnez BYOIP comme cas d'utilisation.
6. Pour le type d'adresse IP, sélectionnez IPv4 ou Dualstack.
7. Pour le pool IPAM, sélectionnez le ou les pools IPAM que vous avez provisionnés via le ou les groupes IPAM et CIDR parmi ceux-ci.

Les étapes suivantes diffèrent du processus BYOIP régional standard et définissent le modèle des services mondiaux :

AWS CLI

Installation ou mise à jour vers la dernière version de la AWS CLI. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Command Line Interface.

1. Récupérez IpamPoolArn le pool IPAM dans lequel vos blocs CIDR ont été provisionnés. Pour plus d'informations, voir Apporter votre propre CIDR IPv4 public à IPAM en utilisant uniquement l'interface de ligne de commande ou AWSImporter votre propre CIDR IPv6 public vers IPAM en utilisant uniquement la CLI. AWS
2. Créez une liste d'adresses IP Anycast avec vos blocs CIDR et votre configuration IPAM :

   Pour IPv4 :

```
aws cloudfront create-anycast-ip-list \
    --name byoip-aip-1 \
    --ip-count 3 \
    --region us-east-1 \
    --ip-address-type ipv4 \
    --ipam-cidr-configs
 '[{"Cidr":"1.1.1.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"2.2.2.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"3.3.3.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"}]'
```

   Pour IPv6 :

```
aws cloudfront create-anycast-ip-list \
    --name byoip-aip-dualstack \
    --ip-count 3 \
    --region us-east-1 \
    --ip-address-type dualstack \
    --ipam-cidr-configs
 '[{"Cidr":"1.1.1.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"2.2.2.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"3.3.3.0/24","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/ipam-
pool-005d58a8aa8147abc"},
{"Cidr":"2600:9000:a100::/48","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a3b7c9e2f41d6789"},
```

```
{"Cidr":"2600:9000:a200::/48","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a3b7c9e2f41d6789"},
{"Cidr":"2600:9000:a300::/48","IpamPoolArn":"arn:aws:ec2::123456789012:ipam-pool/
ipam-pool-0a3b7c9e2f41d6789"}]'
```

> **Note**
>
> Vous ne pouvez pas sélectionner l'adresse IP spécifique dans le pool. CloudFront le fera automatiquement.

Étape 3 : Création d'une CloudFront distribution

En CloudFront effet, vous pouvez suivre les instructions pour créer une distribution standard ou utiliser des distributions multi-locataires.

Étape 4 : Associer aux CloudFront ressources

- Associer une liste IP statique Anycast à une distribution existante
- Associer une liste d'adresses IP statiques Anycast à une nouvelle distribution
- Associer une liste IP statique Anycast à un groupe de connexion

Étape 5 : Préparation à la migration

Pour plus d'informations, consultez l'étape 4 : Préparation de la migration dans le guide de l'utilisateur Amazon VPC.

Étape 6 : Faites la promotion du CIDR dans le monde entier

Pour plus d'informations, consultez l'étape 5 : Promouvoir le CIDR dans le monde entier dans le guide de l'utilisateur Amazon VPC.

Utilisation de gRPC avec des distributions CloudFront

Amazon CloudFront prend en charge gRPC, un framework open source d'appel de procédure à distance (RPC) basé sur celui-ci. HTTP/2 gRPC propose un streaming bidirectionnel et un protocole binaire qui met en mémoire tampon les charges utiles, ce qui le rend adapté aux applications nécessitant des communications à faible latence.

CloudFront reçoit vos requêtes gRPC et les transmet directement à vos origines. Vous pouvez utiliser CloudFront le proxy pour quatre types de services gRPC :

- RPC unaire
- RPC de streaming de serveur
- RPC de streaming client
- Bi-directional RPC en streaming

Comment fonctionne le gRPC dans CloudFront

Pour configurer gRPC dans CloudFront, définissez une origine qui fournit un service gRPC comme origine de votre distribution. Vous pouvez utiliser des origines qui fournissent à la fois des services non GRPC et gRPC. CloudFront détermine si la demande entrante est une demande gRPC ou une HTTP/HTTPS demande basée sur l'`Content-Type`en-tête. Si l'`Content-Type`en-tête d'une demande a la valeur de`application/grpc`, la demande est considérée comme une demande gRPC et la demande CloudFront sera transmise par proxy à votre origine.

> **Note**
>
> Pour permettre à une distribution de gérer les requêtes gRPC, incluez-la HTTP/2 comme l'une des versions HTTP prises en charge et autorisez les méthodes HTTP, notamment. `POST` Votre point de terminaison d'origine gRPC doit être configuré pour prendre en charge le protocole HTTPS, car il CloudFront ne prend en charge que les connexions gRPC sécurisées (). HTTPS-based gRPC ne prend en charge que le protocole HTTPS de bout en bout. Si vous utilisez une origine personnalisée, vérifiez que vos paramètres de Protocole prennent en charge le HTTPS.

Pour activer la prise en charge de gRPC pour votre distribution, procédez comme suit :

1. Mettez à jour le comportement de cache de votre distribution pour autoriser les méthodes HTTP, y compris la méthode `POST`.
2. Après avoir sélectionné la méthode `POST`, cochez la case gRPC qui apparaît.
3. Spécifiez HTTP/2comme l'une des versions HTTP prises en charge.

Pour plus d’informations, consultez les rubriques suivantes :

- Autoriser les requêtes gRPC sur HTTP/2
- GrpcConfigdans le Amazon CloudFront API Reference

Étant donné que gRPC est utilisé uniquement pour le trafic d'API ne pouvant pas être mis en cache, vos configurations de cache n'affecteront pas les demandes gRPC. Vous pouvez utiliser une politique de demande d'origine pour ajouter des en-têtes personnalisés aux demandes gRPC envoyées à votre origine gRPC. Vous pouvez l'utiliser CloudFront pour AWS WAF gérer l'accès à votre distribution gRPC, contrôler les robots et protéger vos applications gRPC contre les exploits Web. CloudFront gRPC prend en charge les fonctionsCloudFront .

En plus du statut HTTPS, vous recevrez le statut grpc-status avec votre réponse gRPC. Pour obtenir la liste des valeurs possibles pour grpc-status, consultez Codes de statut et leur utilisation dans gRPC.

Remarques

gRPC ne prend pas en charge les fonctionnalités suivantes : CloudFront

- réponses aux·erreurs personnalisées
- Le basculement d'origine n'est pas pris en charge avec gRPC, car gRPC utilise une méthode. `POST` CloudFront bascule vers l'origine secondaire uniquement lorsque la méthode HTTP de la demande du spectateur est `GET`, `HEAD`, ou`OPTIONS`.
- CloudFront transmet les requêtes gRPC directement à l'origine et contourne le Regional Edge Cache (REC). Étant donné que gRPC contourne le REC, gRPC ne prend pas en charge Lambda@Edge ni Origin Shield.
- gRPC ne prend pas en charge les règles d'inspection du corps des AWS WAF demandes. Si vous avez activé ces règles sur l'ACL web d'une distribution, toute demande utilisant gRPC ignorera les règles d'inspection du corps de la demande. Toutes les autres règles AWS WAF continueront de s'appliquer. Pour plus d'informations, consultez Enable AWS WAF pour les distributions.

Travailler avec des ressources partagées dans CloudFront

Amazon CloudFront s'intègre à AWS Resource Access Manager (AWS RAM) pour permettre le partage des ressources. AWS RAM vous permet de partager certaines CloudFront ressources avec d'autres personnes Comptes AWS ou via AWS Organizations. Avec AWS RAM, vous pouvez partager des ressources dont vous êtes propriétaire en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent être :

- Spécifique Comptes AWS à l'intérieur ou à l'extérieur de son organisation dans AWS Organizations
- Une unité organisationnelle au sein de son organisation en AWS Organizations
- L'ensemble de son organisation en AWS Organizations

Pour plus d'informations à ce sujet AWS RAM, consultez le Guide de AWS RAM l'utilisateur.

Cette rubrique explique comment partager les ressources que vous possédez et comment utiliser les ressources qui sont partagées avec vous.

Table des matières

- Conditions préalables au partage des ressources
- Partage d'une origine VPC
- Utilisation d'une origine VPC partagée
- Identifier une origine VPC partagée
- Annuler le partage d'une origine VPC partagée
- Responsabilités et autorisations pour les origines de VPC partagées
- Facturation et mesures
- Quotas de ressources partagées

Conditions préalables au partage des ressources

- Vous devez disposer de la politique AWSRAMDefaultPermissionCloudFront gérée pour accorder un accès en lecture seule au partage de ressources. Pour plus d’informations, consultez AWSRAMDefaultPermissionCloudFront.

- Pour partager une origine VPC, vous devez en être propriétaire dans votre Compte AWS. Cela signifie que la ressource doit être allouée ou provisionnée dans votre compte. Vous ne pouvez pas partager une ressource qui a été partagée avec vous.
- Pour partager une ressource avec votre organisation ou une unité organisationnelle au sein de AWS Organizations, vous devez activer le partage avec AWS Organizations. Pour plus d'informations, consultez Activation du partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Partage d'une origine VPC

> **Note**
>
> Prend actuellement en CloudFront charge le partage des origines des VPC. Si vous n'en avez pas encore créé un, consultezRestriction de l'accès avec les origines de VPC.

Lorsque vous partagez une origine VPC que vous possédez avec d'autres Comptes AWS personnes, vous leur permettez d'utiliser cette ressource comme origine pour leurs CloudFront distributions.

Pour partager une origine VPC, vous devez l'ajouter à un partage de ressources. Un partage de ressources est une ressource AWS RAM qui vous permet de partager vos ressources entre des Comptes AWS.

Un partage de ressources spécifie les éléments suivants :

- Les ressources que vous souhaitez partager
- Les consommateurs avec lesquels ils sont partagés
- La politique gérée du service qui détermine les autorisations d'accès aux ressources

Lorsque vous partagez une origine VPC à l'aide de la CloudFront console, vous l'ajoutez à un partage de ressources existant. Si vous n'avez pas encore de partage de ressources, vous pouvez en créer un lorsque vous partagez une origine VPC depuis la CloudFront console. Vous pouvez également utiliser la AWS RAM console ou AWS CLI en créer une séparément.

Vous pouvez partager les origines du VPC avec d'autres utilisateurs Comptes AWS et AWS Organizations.

- Si vous partagez la ressource avec une AWS organisation, tous les consommateurs de cette organisation spécifique sont autorisés à accéder à l'origine du VPC.
- Si vous partagez des ressources avec une Compte AWS organisation dont vous ne faites pas partie, les consommateurs recevront une invitation les invitant à accepter le partage de ressources. Une fois acceptés, ils peuvent utiliser l'origine du VPC.

Vous pouvez partager une origine VPC que vous possédez à l'aide de la CloudFront console, de la AWS RAM console ou du AWS CLI.

Pour créer un partage de ressources à l'aide de la CloudFront console

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez VPC origins.
3. Sélectionnez une ou plusieurs ressources et choisissez Partager l'origine du VPC.
4. Choisissez Créer une ressource.
5. Dans le champ Nom, entrez le nom du partage de ressources.
6. Pour Type principal, sélectionnez l'une des options suivantes :

   - Compte AWS— Accordez l'accès à un accès spécifique Compte AWS.
   - Unité organisationnelle : accordez l'accès à une unité organisationnelle (UO) spécifique.
   - Organisation : accordez l'accès à l'ensemble de votre organisation, y compris à ses unités d'organisation enfants et Comptes AWS.

   a. Si vous le souhaitez Compte AWS, entrez le numéro d'identification du compte. Vous pouvez choisir Ajouter un nouveau compte pour en ajouter jusqu'à 5 Comptes AWS.
   b. Si vous avez choisi Unité organisationnelle, entrez l'ARN de l'unité OU. Vous ne pouvez saisir qu'une seule unité d'organisation.
   c. Si vous avez choisi Organisation, entrez l'ARN de l'organisation. Vous ne pouvez inscrire qu'une seule organisation.
7. Choisissez Partager les ressources.

   Par défaut, CloudFront applique la politique AWSRAMDefaultPermissionCloudFront AWS gérée au partage de ressources. Cette politique autorise les actions en lecture seule sur le partage de ressources, de sorte que les comptes consommateurs ne peuvent pas mettre à jour ou

supprimer la ressource partagée. Vous ne pouvez ni modifier ni supprimer cette politique du partage de ressources.

> **Tip**
>
> Après avoir créé le partage de ressources, vous pouvez en ajouter Comptes AWS d'autres depuis la AWS RAM console. Pour plus d'informations, voir Mettre à jour un partage de ressources dans la AWS RAM dans le Guide de AWS RAM l'utilisateur.

Pour partager une origine VPC dont vous êtes propriétaire à l'aide de la console CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez VPC origins.
3. Sélectionnez une ressource et choisissez Partager l'origine du VPC.
4. Sur la page Partager l'origine du VPC, vous pouvez sélectionner un partage de ressources existant auquel vous souhaitez ajouter cette origine VPC.
5. Choisissez Partager la ressource.

   Sur la page détaillée des ressources, sous Partagé avec, vous pouvez voir que l'origine de votre VPC est partagée avec les informations suivantes :

   - Noms des partages de ressources
   - État du partage
   - Date de dernière modification

Une fois que vous avez créé et partagé le partage de ressources avec les comptes utilisateurs, ceux-ci disposent de 12 heures pour accepter l'invitation. Pour plus d'informations, voir Accepter et rejeter les invitations à partager des ressources dans le Guide de l'AWS RAM utilisateur.

> **Important**
>
> Pour permettre aux comptes consommateurs d'utiliser l'origine de votre VPC pour leur CloudFront distribution, vous devez également leur fournir le point de terminaison Elastic Load Balancing ou Amazon EC2 de l'origine du VPC.

Pour partager une origine VPC dont vous êtes propriétaire à l'aide du AWS RAM console

Créez un partage de ressources, puis choisissez les CloudFront ressources que vous souhaitez y ajouter. Pour plus d'informations, consultez la section Création d'un partage de ressources dans le Guide de AWS RAM l'utilisateur.

Pour partager une origine VPC dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande create-resource-share.

Utilisation d'une origine VPC partagée

Pour utiliser une origine VPC partagée, le compte qui reçoit l'invitation doit accepter le partage de ressources. Vous pouvez le faire en accédant à la AWS Resource Access Manager console dans la région USA Est (Virginie du Nord) et en acceptant toutes les demandes en attente dans l'onglet En attente. Pour plus d'informations, consultez la section Acceptation des ressources partagées dans le Guide de AWS RAM l'utilisateur.

Une fois que vous avez accepté le partage des ressources, vous pouvez utiliser l'origine du VPC comme origine pour vos CloudFront distributions.

Pour utiliser une origine VPC partagée

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, pour Distributions, effectuez l'une des opérations suivantes :
   - Pour une nouvelle distribution, choisissez Créer une distribution.
   - Pour une distribution existante, choisissez l'ID de distribution.
3. Pour le type d'origine, choisissez l'origine du VPC, puis spécifiez l'origine du VPC qui a été partagée avec vous.
4. Pour le point de terminaison d'origine du VPC, entrez le nom DNS privé de votre instance Amazon EC2 ou de votre équilibreur de charge Elastic Load Balancing, ou du domaine d'origine. Si vous ne possédez pas encore cette valeur, vous devez l'obtenir auprès du propriétaire de Compte AWS l'origine du VPC. Si vous ne possédez pas encore ce point de terminaison, vous pouvez l'obtenir auprès du Compte AWS propriétaire de l'origine du VPC.
5. Suivez les autres étapes de la console pour créer ou mettre à jour votre distribution.

Identifier une origine VPC partagée

Les propriétaires et les consommateurs peuvent identifier les origines des VPC partagés à l'aide de la CloudFront console et AWS CLI.

Pour identifier l'origine d'un VPC partagé à l'aide de la console CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez VPC origins. Vous pouvez utiliser la colonne Owner ID pour identifier la Compte AWS personne à laquelle appartient la ressource.
3. Sélectionnez une ressource.
4. Sur la page détaillée des ressources, sous Partagé avec, vous pouvez voir que l'origine de votre VPC est partagée avec les informations suivantes :

   - Noms des partages de ressources
   - État du partage
   - Date de dernière modification

Annuler le partage d'une origine VPC partagée

Lorsque vous annulez le partage d'une ressource, les Comptes AWS (comptes consommateurs) ne peuvent plus utiliser cette ressource pour de nouvelles distributions ou mettre à jour des distributions existantes.

> **Note**
>
> Si vous annulez le partage d'une ressource, les distributions existantes qui utilisent toujours cette ressource restent actives et continueront à gérer le trafic. Cependant, ces distributions ne peuvent pas être modifiées tant que la ressource non partagée n'est pas supprimée en tant qu'origine. Nous vous recommandons de vous assurer que tous les comptes consommateurs cessent d'utiliser la ressource non partagée avant de l'annuler.

Pour annuler le partage d'une origine VPC partagée dont vous êtes propriétaire, vous devez la supprimer du partage de ressources. Vous pouvez le faire à l'aide de la CloudFront AWS RAM console, de la console ou du AWS CLI.

Pour annuler le partage d'une origine VPC partagée dont vous êtes propriétaire à l'aide de la console CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez VPC origins.
3. Sélectionnez une ressource et choisissez Annuler le partage.
4. Vérifiez les détails dans la boîte de dialogue Annuler le partage de la ressource, puis choisissez Annuler le partage. Les personnes principales répertoriées n'auront plus accès à votre ressource partagée.

Pour annuler le partage d'une origine VPC partagée dont vous êtes propriétaire à l'aide du AWS RAM console

Consultez Mise à jour d’un partage de ressources dans le Guide de l’utilisateur AWS RAM .

Pour annuler le partage d'une origine VPC partagée dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Responsabilités et autorisations pour les origines de VPC partagées

Autorisations accordées aux propriétaires

En tant que compte propriétaire de la ressource, assurez-vous que tous les comptes consommateurs cessent d'utiliser la ressource avant d'annuler le partage ou de la supprimer.

Autorisations accordées aux consommateurs

Les comptes consommateurs peuvent utiliser des ressources partagées comme sources pour leurs CloudFront distributions, mais ils ne peuvent ni modifier ni supprimer les ressources. Par défaut, la politique AWSRAMDefaultPermissionCloudFront AWS gérée est appliquée au partage de ressources dans le compte de partage (le compte propriétaire de la ressource).

AWSRAMDefaultPermissionCloudFront

Lorsque vous créez un partage de ressources dans CloudFront, CloudFront utilise la politique AWSRAMDefaultPermissionCloudFront AWS gérée et l'applique à votre partage de ressources.

Cette politique accorde des autorisations en lecture seule aux CloudFront ressources qui peuvent être partagées entre le propriétaire de la ressource et le compte utilisateur.

Pour plus d'informations sur la gestion des autorisations dans AWS RAM, voir Gestion des autorisations AWS RAM dans le Guide de AWS Resource Access Manager l'utilisateur.

Facturation et mesures

Le partage des origines des VPC avec d'autres Comptes AWS utilisateurs est gratuit. Les coûts d'utilisation du trafic pour une distribution utilisant une origine VPC partagée seront versés au compte consommateur propriétaire de la distribution.

Quotas de ressources partagées

CloudFront utilise les mêmes quotas de partage des ressources que ceux spécifiés par AWS RAM. À partir de la CloudFront console, vous pouvez ajouter jusqu'à 5 Comptes AWS, 1 unité d'organisation ou 1 organisation. Pour en ajouter d'autres, utilisez la AWS RAM console ou AWS RAM l'API.

Pour plus d’informations, consultez Quotas de service pour AWS RAM dans le Guide de l’utilisateur AWS RAM .

Mise en cache et disponibilité

Vous pouvez l'utiliser CloudFront pour réduire le nombre de demandes auxquelles votre serveur d'origine doit répondre directement. Grâce à la CloudFront mise en cache, un plus grand nombre d'objets sont servis à partir d'emplacements CloudFront périphériques, plus proches de vos utilisateurs. Cela réduit la charge sur votre serveur d'origine et la latence.

Plus le nombre de requêtes CloudFront pouvant être traitées à partir des caches périphériques est élevé, moins CloudFront il y a de requêtes de spectateurs à transmettre à votre source pour obtenir la dernière version ou une version unique d'un objet. Pour optimiser et CloudFront adresser le moins de requêtes possible à votre origine, pensez à utiliser un CloudFront Origin Shield. Pour plus d'informations, consultez Utiliser Amazon CloudFront Origin Shield.

La proportion de demandes traitées directement depuis le CloudFront cache par rapport à l'ensemble des demandes est appelée taux d'accès au cache. Vous pouvez consulter le pourcentage de demandes des spectateurs qui sont des succès, des échecs et des erreurs dans la CloudFront console. Pour plus d'informations, consultez Afficher les rapports statistiques du CloudFront cache.

Un certain nombre de facteurs influencent le taux d'accès au cache. Vous pouvez ajuster CloudFront la configuration de votre distribution pour améliorer le taux d'accès au cache en suivant les instructions de la sectionAugmenter la proportion de demandes traitées directement depuis les CloudFront caches (taux d'accès au cache).

Pour en savoir plus sur l'ajout et la suppression du contenu que vous CloudFront souhaitez diffuser, consultezAjouter, supprimer ou remplacer le contenu qui CloudFront distribue.

Rubriques

- Augmenter la proportion de demandes traitées directement depuis les CloudFront caches (taux d'accès au cache)
- Utiliser Amazon CloudFront Origin Shield
- Optimisez la haute disponibilité grâce au basculement CloudFront d'origine
- Gestion de la durée de conservation de contenu dans le cache (expiration)
- Mise en cache de contenu basée sur les paramètres de chaîne de requête
- Mise en cache de contenu basée sur des cookies
- Mise en cache de contenu basée sur des en-têtes de demandes

Augmenter la proportion de demandes traitées directement depuis les CloudFront caches (taux d'accès au cache)

Vous pouvez améliorer les performances en augmentant la proportion de demandes de vos spectateurs qui sont traitées directement depuis le CloudFront cache au lieu d'être transmises à vos serveurs d'origine pour le contenu. Ce processus est appelé « amélioration du taux d'accès au cache ».

Les sections suivantes expliquent comment améliorer votre taux d'accès au cache.

Rubriques

- Spécifiez la durée de mise CloudFront en cache de vos objets
- Utilisation d'Origin Shield
- Mise en cache basée sur les paramètres de chaîne de requête
- Mise en cache basée sur des valeurs de cookie
- Mise en cache basée sur des valeurs d'en-tête
- Supprimer l'en-tête Accept-Encoding lorsqu'une compression n'est pas nécessaire
- Diffusion de contenu multimédia via HTTP

Spécifiez la durée de mise CloudFront en cache de vos objets

Pour augmenter le taux d'accès de votre cache, vous pouvez configurer votre origine pour ajouter une directive Cache-Control max-age à vos objets et spécifier la valeur la plus longue possible pour. `max-age` Plus la durée du cache est courte, plus les requêtes sont CloudFront envoyées fréquemment à votre origine pour déterminer si un objet a changé et pour obtenir la dernière version. Vous pouvez compléter `max-age` avec les directives `stale-while-revalidate` et `stale-if-error` pour améliorer davantage le taux d'accès au cache sous certaines conditions. Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Utilisation d'Origin Shield

CloudFront Origin Shield peut contribuer à améliorer le taux d'accès au cache de votre CloudFront distribution, car il fournit une couche de mise en cache supplémentaire devant votre origine. Lorsque vous utilisez Origin Shield, toutes les requêtes de toutes les couches de CloudFront mise en cache

adressées à votre origine proviennent d'un seul emplacement. CloudFront peut récupérer chaque objet à l'aide d'une seule demande d'origine depuis Origin Shield, et toutes les autres couches du CloudFront cache (emplacements périphériques et caches périphériques régionaux) peuvent récupérer l'objet depuis Origin Shield.

Pour plus d'informations, consultez Utiliser Amazon CloudFront Origin Shield.

Mise en cache basée sur les paramètres de chaîne de requête

Si vous configurez CloudFront la mise en cache en fonction des paramètres de chaîne de requête, vous pouvez améliorer la mise en cache en procédant comme suit :

- Configurez CloudFront pour ne transmettre que les paramètres de chaîne de requête pour lesquels votre origine renverra des objets uniques.
- Utilisez la même casse (majuscules ou minuscules) pour toutes les instances du même paramètre. Par exemple, si une demande contient `parameter1=A` et qu'une autre en contient`parameter1=a`, CloudFront transmet des demandes distinctes à votre origine lorsqu'une demande contient `parameter1=A` et quand une demande contient`parameter1=a`. CloudFront met ensuite en cache séparément les objets correspondants renvoyés séparément par votre origine, même s'ils sont identiques. Si vous utilisez uniquement `A` ou `a`, CloudFront réachemine moins de requêtes vers votre origine.
- Listez les paramètres dans le même ordre. Comme avec les différences de casse, si une requête pour un objet contient la chaîne de requête `parameter1=a&parameter2=b` et une autre requête contient `parameter2=b&parameter1=a`, CloudFront réachemine les deux requêtes à votre origine et met en cache les objets correspondants séparément même s'ils sont identiques. Si vous utilisez toujours le même ordre pour les paramètres, CloudFront vous transmettez moins de demandes à votre origine.

Pour plus d'informations, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête. Si vous souhaitez consulter les chaînes de requête qui CloudFront sont transmises à votre origine, consultez les valeurs dans la `cs-uri-query` colonne de vos fichiers CloudFront journaux. Pour plus d'informations, consultez Journaux d'accès (journaux standard).

Mise en cache basée sur des valeurs de cookie

Si vous configurez CloudFront la mise en cache en fonction des valeurs des cookies, vous pouvez améliorer la mise en cache en procédant comme suit :

- Configurez CloudFront pour transférer uniquement les cookies spécifiés au lieu de transférer tous les cookies. Pour les cookies que vous configurez pour qu' CloudFront ils soient redirigés vers votre site d'origine, CloudFront ils transmettent toutes les combinaisons de nom et de valeur des cookies. Il met ensuite en cache séparément les objets renvoyés par votre origine, même s'ils sont tous identiques.

  Supposons par exemple que les utilisateurs incluent deux cookies dans chaque demande, que chaque cookie ait trois valeurs possibles et que toutes les combinaisons de valeurs de cookies soient possibles. CloudFront transmet jusqu'à neuf demandes différentes à votre source pour chaque objet. Si votre origine renvoie différentes versions d'un objet sur la base d'un seul des cookies, cela signifie qu' CloudFront il transmet plus de demandes que nécessaire à votre origine et met inutilement en cache plusieurs versions identiques de l'objet.
- Créez des comportements de cache distincts pour le contenu statique et dynamique, et configurez CloudFront pour transférer les cookies vers votre origine uniquement pour le contenu dynamique.

  Supposons, par exemple, que vous n'ayez qu'un seul comportement de cache pour votre distribution et que vous utilisiez cette distribution à la fois pour le contenu dynamique, tel que `.js` les fichiers, et pour `.css` les fichiers qui changent rarement. CloudFront met en cache des versions distinctes de vos `.css` fichiers en fonction des valeurs des cookies, de sorte que chaque emplacement CloudFront périphérique transmet une demande à votre origine pour chaque nouvelle valeur de cookie ou combinaison de valeurs de cookie.

  Supposons que vous créiez un comportement de cache dont le modèle de chemin est `*.css` défini et que le comportement ne soit pas mis en cache en fonction des valeurs des cookies. Dans ce cas, CloudFront transfère les demandes de `.css` fichiers à votre origine uniquement pour la première demande qu'un emplacement périphérique reçoit pour un `.css` fichier donné et pour la première demande après l'expiration d'un `.css` fichier.
- Si possible, créez des comportements de cache distincts pour les contenus dynamiques pour lesquels les valeurs de cookie sont uniques pour chaque utilisateur (comme un ID utilisateur) et les contenus dynamiques qui varient selon un plus petit nombre de valeurs uniques.

Pour plus d’informations, consultez Mise en cache de contenu basée sur des cookies. Si vous souhaitez consulter les cookies qui redirigent CloudFront vers votre site d'origine, consultez les valeurs dans la `cs(Cookie)` colonne de vos fichiers CloudFront journaux. Pour plus d’informations, consultez Journaux d'accès (journaux standard).

Mise en cache basée sur des valeurs d'en-tête

Si vous configurez CloudFront la mise en cache en fonction des en-têtes de demande, vous pouvez améliorer la mise en cache en procédant comme suit :

- Configurez CloudFront pour transférer et mettre en cache uniquement en fonction des en-têtes spécifiés au lieu de transférer et de mettre en cache en fonction de tous les en-têtes. Pour les en-têtes que vous spécifiez, CloudFront transfère chaque combinaison de nom et de valeur d'en-tête. Il met ensuite en cache séparément les objets que votre origine renvoie, même s'ils sont tous identiques.

  > **Note**
  >
  > CloudFront transmet toujours à votre origine les en-têtes spécifiés dans les rubriques suivantes :
  >
  > - Comment CloudFront traiter et transférer les demandes vers votre serveur d'origine Amazon S3 > en-têtes de requête HTTP qui CloudFront suppriment ou mettent à jour
  > - Comment CloudFront traiter et transférer les demandes vers votre serveur d'origine personnalisé > En-têtes et CloudFront comportement des requêtes HTTP (origines personnalisées et Amazon S3)

  Lorsque vous configurez CloudFront la mise en cache en fonction des en-têtes de demande, vous ne modifiez pas les en-têtes qui CloudFront sont transférés, mais uniquement si les objets sont mis en CloudFront cache en fonction des valeurs d'en-tête.
- Essayez d'éviter d'effectuer la mise en cache en fonction d'en-têtes de demande qui ont des nombres importants de valeurs uniques.

  Par exemple, si vous souhaitez diffuser différentes tailles d'image en fonction de l'appareil de l'utilisateur, ne configurez CloudFront pas la mise en cache en fonction de l'`User-Agent`en-tête, qui comporte un très grand nombre de valeurs possibles. Configurez plutôt CloudFront pour mettre en cache en fonction des en-têtes du CloudFront type de périphérique`CloudFront-Is-Desktop-Viewer`,`CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer` et. `CloudFront-Is-Tablet-Viewer` De plus, si vous renvoyez la même version de l'image pour des tablettes et des ordinateurs de bureau, transmettez uniquement l'en-tête `CloudFront-Is-Tablet-Viewer`, pas l'en-tête `CloudFront-Is-Desktop-Viewer`.

Pour plus d'informations, consultez Mise en cache de contenu basée sur des en-têtes de demandes.

Supprimer l'en-tête **`Accept-Encoding`** lorsqu'une compression n'est pas nécessaire

Si la compression n'est pas activée, parce que l'origine ne la prend pas en charge, CloudFront ne le prend pas en charge ou parce que le contenu n'est pas compressible, vous pouvez augmenter le taux d'accès du cache en associant un comportement de cache dans votre distribution à une origine qui définit comme suit : Custom Origin Header

- Header name (Nom de l'en-tête: `Accept-Encoding`
- Header value (Valeur de l'en-tête) : (laisser vide)

Lorsque vous utilisez cette configuration, CloudFront supprime l'`Accept-Encoding`en-tête de la clé de cache et n'inclut pas l'en-tête dans les demandes d'origine. Cette configuration s'applique à tout le CloudFront contenu diffusé à partir de cette origine.

Diffusion de contenu multimédia via HTTP

Pour plus d'informations sur l'optimisation du contenu vidéo à la demande (VOD) et en streaming, consultez Vidéo à la demande et diffusion en direct avec CloudFront.

Utiliser Amazon CloudFront Origin Shield

CloudFront Origin Shield est une couche supplémentaire de l'infrastructure de mise en CloudFront cache qui permet de minimiser la charge de votre origine, d'améliorer sa disponibilité et de réduire ses coûts d'exploitation. Avec CloudFront Origin Shield, vous bénéficiez des avantages suivants :

Un meilleur taux d'accès au cache

Origin Shield peut contribuer à améliorer le taux de réussite du cache de votre CloudFront distribution, car il fournit une couche de mise en cache supplémentaire devant votre source d'origine. Lorsque vous utilisez Origin Shield, toutes les demandes provenant de toutes les couches de CloudFront mise en cache adressées à votre origine passent par Origin Shield, ce qui augmente le risque d'accès au cache. Les demandes effectuées dans la même région que votre pays d'origine contourneront Origin Shield. CloudFrontpeut récupérer chaque objet avec une seule demande d'origine envoyée par Origin Shield à votre origine, et toutes les autres couches

du CloudFront cache (emplacements périphériques et caches périphériques régionaux) peuvent récupérer l'objet depuis Origin Shield.

Une charge d'origine réduite

La couche Origin Shield peut réduire davantage le nombre de demandes simultanées envoyées à votre origine pour le même objet. Les demandes de contenu ne se trouvant pas dans le cache d'Origin Shield sont consolidées avec d'autres demandes liées au même objet, ce qui permet qu'une seule demande soit envoyée à votre origine. En réduisant le nombre de demandes gérées par votre origine, vous préservez la disponibilité de cette dernière pendant les pics de charge ou les pointes de trafic inattendues, mais vous réduisez également les coûts pour des opérations telles que l'empaquetage juste à temps, les transformations d'image et le transfert de données sortantes.

De meilleures performances réseau

Lorsque vous activez Origin Shield dans la AWS région où la latence par rapport à votre origine est la plus faible, vous pouvez obtenir de meilleures performances réseau. Pour les origines situées dans une AWS région, le trafic CloudFront réseau reste sur le CloudFront réseau à haut débit jusqu'à votre point d'origine. Pour les origines extérieures AWS, le trafic CloudFront réseau reste sur le CloudFront réseau jusqu'à Origin Shield, qui dispose d'une connexion à faible latence avec votre point d'origine.

Vous encourez des frais supplémentaires pour l’utilisation d’Origin Shield. Pour en savoir plus, consultez PricingCloudFront (Tarification).

> **Note**
>
> Origin Shield n’est pas compatible avec les demandes gRPC. Si Origin Shield est activé sur une distribution prenant en charge gRPC, les demandes gRPC continueront de fonctionner. Cependant, les demandes seront transmises directement à l’origine gRPC sans passer par Origin Shield. Pour plus d’informations, consultez Utilisation de gRPC avec des distributions CloudFront.

Rubriques

- Cas d'utilisation pour Origin Shield
- Cliquez sur l'onglet AWS Région pour Origin Shield

- Activer Origin Shield
- Estimation des frais liés à Origin Shield
- Haute disponibilité d'Origin Shield
- Comment Origin Shield interagit avec les autres fonctionnalités CloudFront

Cas d'utilisation pour Origin Shield

CloudFront Origin Shield peut être utile dans de nombreux cas d'utilisation, notamment les suivants :

- Utilisateurs répartis dans différentes régions géographiques
- Origines fournissant un empaquetage juste-à-temps pour le streaming en direct ou le traitement d'images à la volée
- On-premises origines soumises à des contraintes de capacité ou de bande passante
- Charges de travail utilisant plusieurs réseaux de diffusion de contenu

Il est possible qu'Origin Shield ne soit pas adapté dans certains cas, par exemple pour du contenu dynamique transmis par proxy à l'origine, du contenu avec une mise en cache faible ou du contenu rarement demandé.

Les sections suivantes expliquent les avantages d'Origin Shield pour les cas d'utilisation suivants.

Cas d’utilisation

- Utilisateurs dans des régions géographiques différentes
- Réseaux de diffusion de contenu multiples

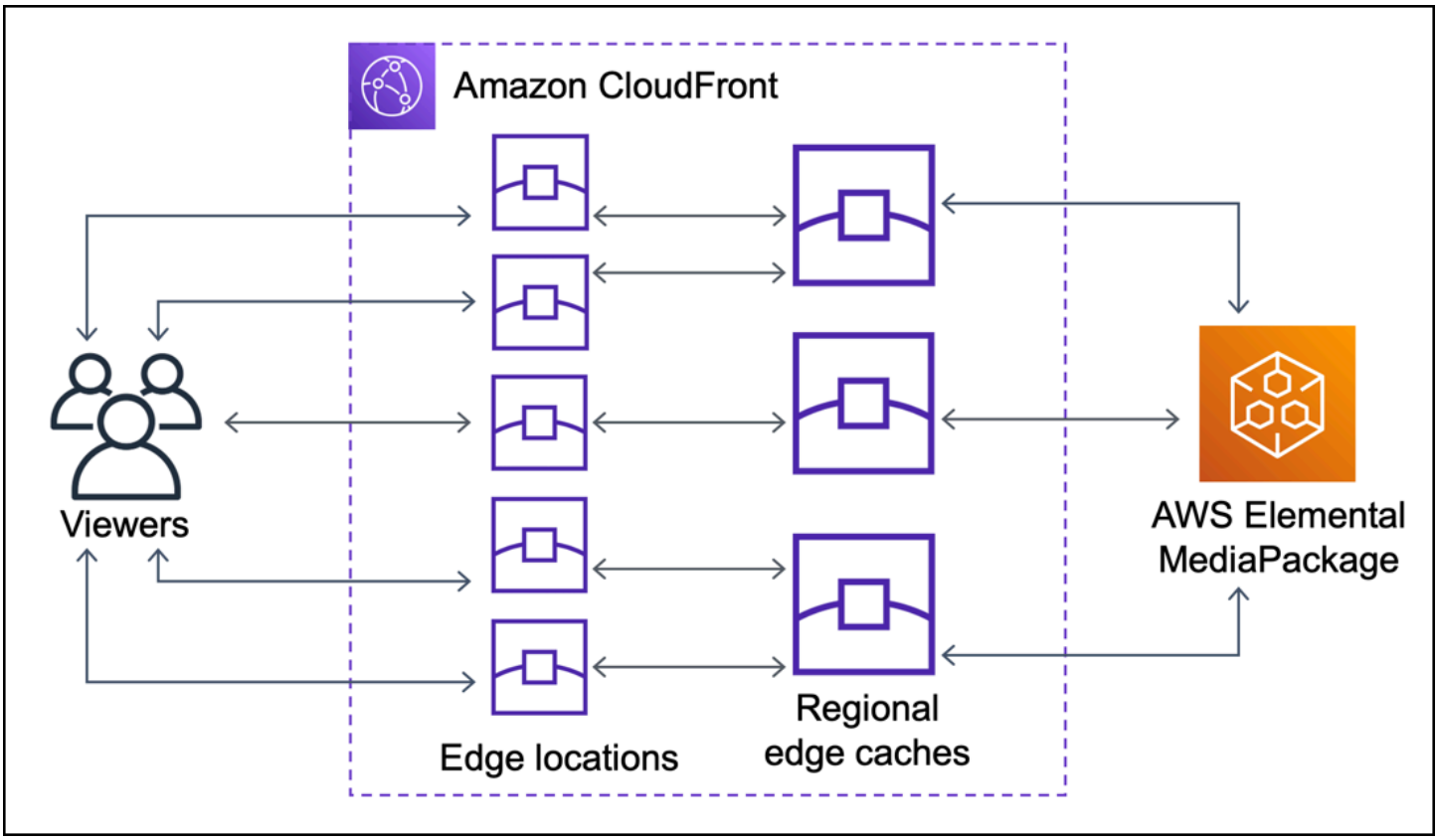
Utilisateurs dans des régions géographiques différentes

Avec Amazon CloudFront, vous bénéficiez par nature d'une charge réduite sur votre source, car les demandes qui CloudFront peuvent être envoyées depuis le cache ne sont pas transmises à votre origine. Outre le réseau CloudFront mondial d'emplacements périphériques, les caches périphériques régionaux servent de couche de mise en cache de niveau intermédiaire pour fournir des accès au cache et consolider les demandes d'origine pour les utilisateurs des régions géographiques voisines. Les demandes des utilisateurs sont d'abord acheminées vers un emplacement périphérique CloudFront voisin et, si l'objet n'est pas mis en cache dans cet emplacement, la demande est envoyée à un cache périphérique régional.

Lorsque les utilisateurs se trouvent dans des régions géographiques différentes, les demandes peuvent être acheminées via différents caches périphériques régionaux, chacun pouvant envoyer une demande à votre origine pour le même contenu. Avec Origin Shield, vous disposez d'une couche supplémentaire de mise en cache entre les caches périphériques régionaux et votre origine. Toutes les demandes provenant de tous les caches périphériques régionaux passent par Origin Shield, réduisant encore la charge sur votre origine. Les diagrammes suivants illustrent ce concept. Dans les diagrammes suivants, l'origine est AWS Elemental MediaPackage.

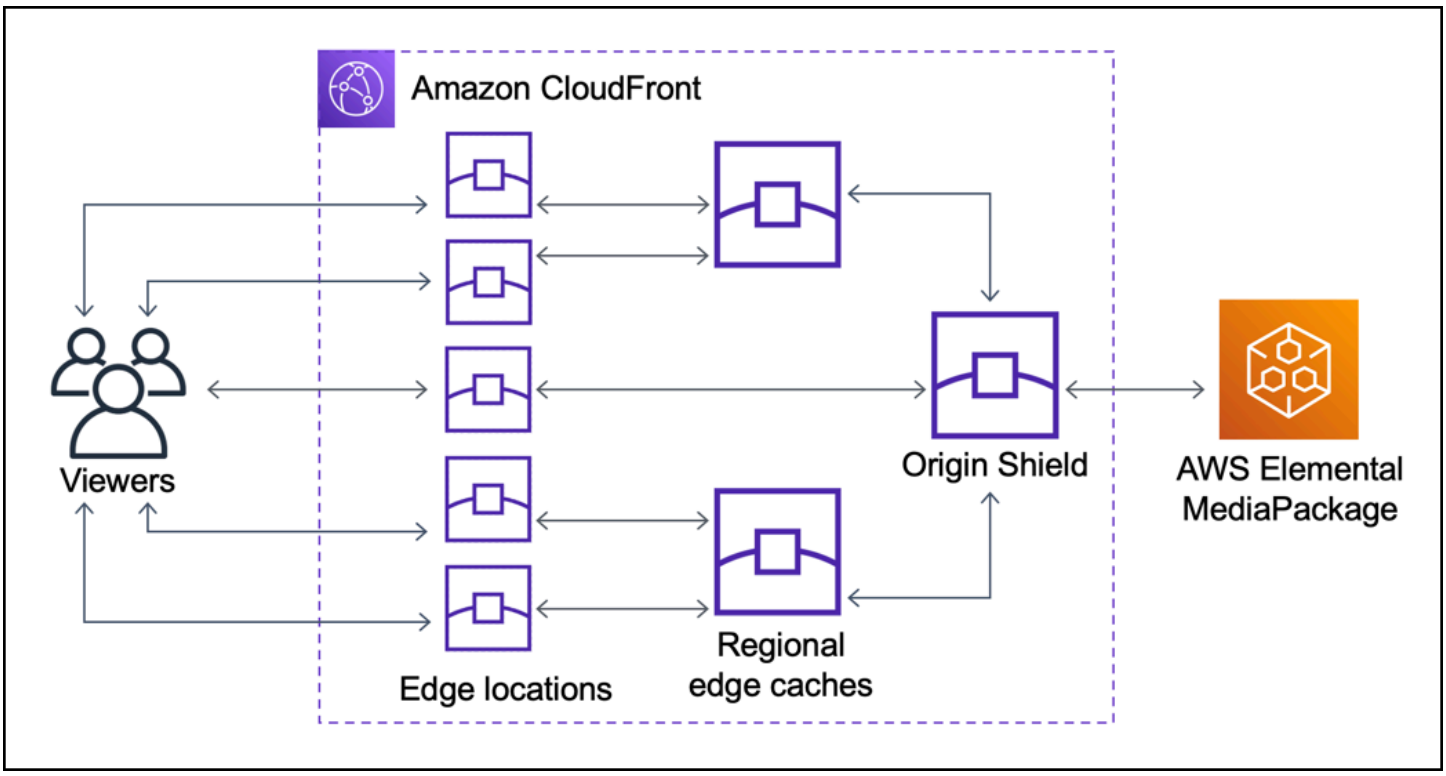
Sans Origin Shield

Sans Origin Shield, votre origine peut recevoir des demandes en double pour le même contenu, comme le montre le diagramme suivant.



Avec Origin Shield

L'utilisation d'Origin Shield permet de réduire la charge sur votre origine, comme le montre le diagramme suivant.



Réseaux de diffusion de contenu multiples

Pour diffuser des événements vidéo en direct ou du contenu populaire à la demande, vous pouvez utiliser plusieurs réseaux de diffusion de contenu. L'utilisation de plusieurs réseaux de diffusion de contenu peut offrir certains avantages, mais cela signifie également que votre origine peut recevoir de nombreuses demandes en double pour le même contenu, chacune provenant de réseaux différents ou d'emplacements différents au sein du même réseau de diffusion de contenu. Ces demandes redondantes peuvent nuire à la disponibilité de votre origine ou entraîner des coûts d'exploitation supplémentaires pour des processus tels que l'empaquetage juste-à-temps ou le transfert de données sortantes vers Internet.

Lorsque vous associez Origin Shield à l'utilisation de votre CloudFront distribution comme point d'origine pour d'autres CDN, vous pouvez bénéficier des avantages suivants :

- Un nombre moins important de demandes redondantes reçues par votre origine, ce qui contribue à réduire les effets négatifs de l'utilisation de plusieurs réseaux de diffusion de contenu.
- Une clé de cache commune sur les réseaux de diffusion de contenu et une gestion centralisée des fonctions liées à l'origine.
- Amélioration des performances réseau Le trafic réseau provenant d'autres CDN est interrompu à un emplacement CloudFront périphérique proche, ce qui peut provoquer un accès depuis le cache

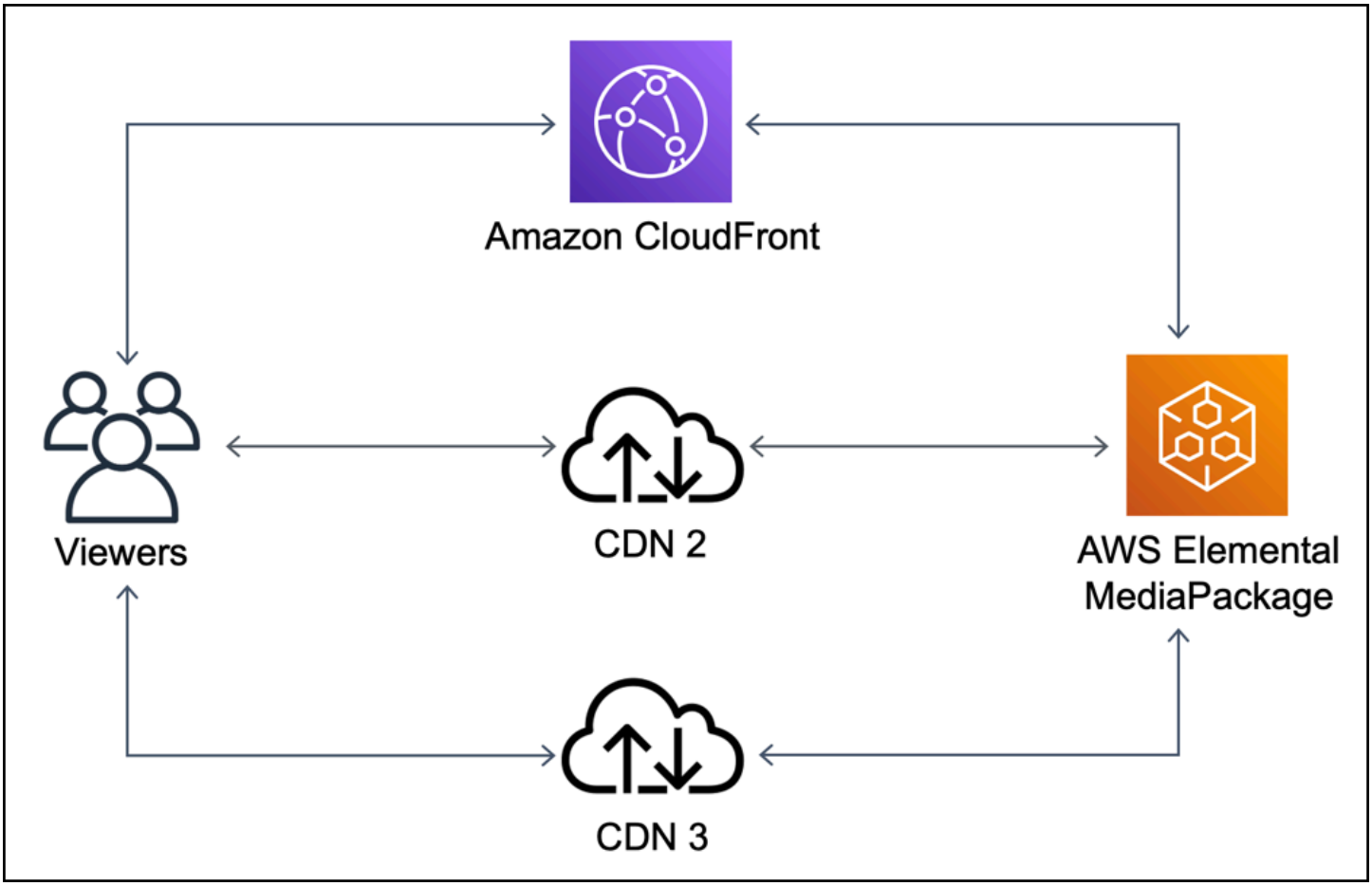
local. Si l'objet demandé ne se trouve pas dans le cache de localisation périphérique, la demande envoyée à l'origine reste sur le CloudFront réseau jusqu'à Origin Shield, qui fournit un débit élevé et une faible latence à l'origine. Si l'objet demandé se trouve dans le cache d'Origin Shield, la demande à votre origine est entièrement évitée.

> **Important**
>
> Si vous souhaitez utiliser Origin Shield dans une architecture multi-CDN et bénéficier de tarifs réduits, contactez-nous ou contactez votre représentant AWS commercial pour plus d'informations. Des frais supplémentaires peuvent s'appliquer.

Les diagrammes suivants montrent comment cette configuration peut aider à réduire la charge sur votre origine lorsque vous diffusez des événements vidéo populaires en direct avec plusieurs réseaux de diffusion de contenu. Dans les diagrammes suivants, l'origine est AWS Elemental MediaPackage.

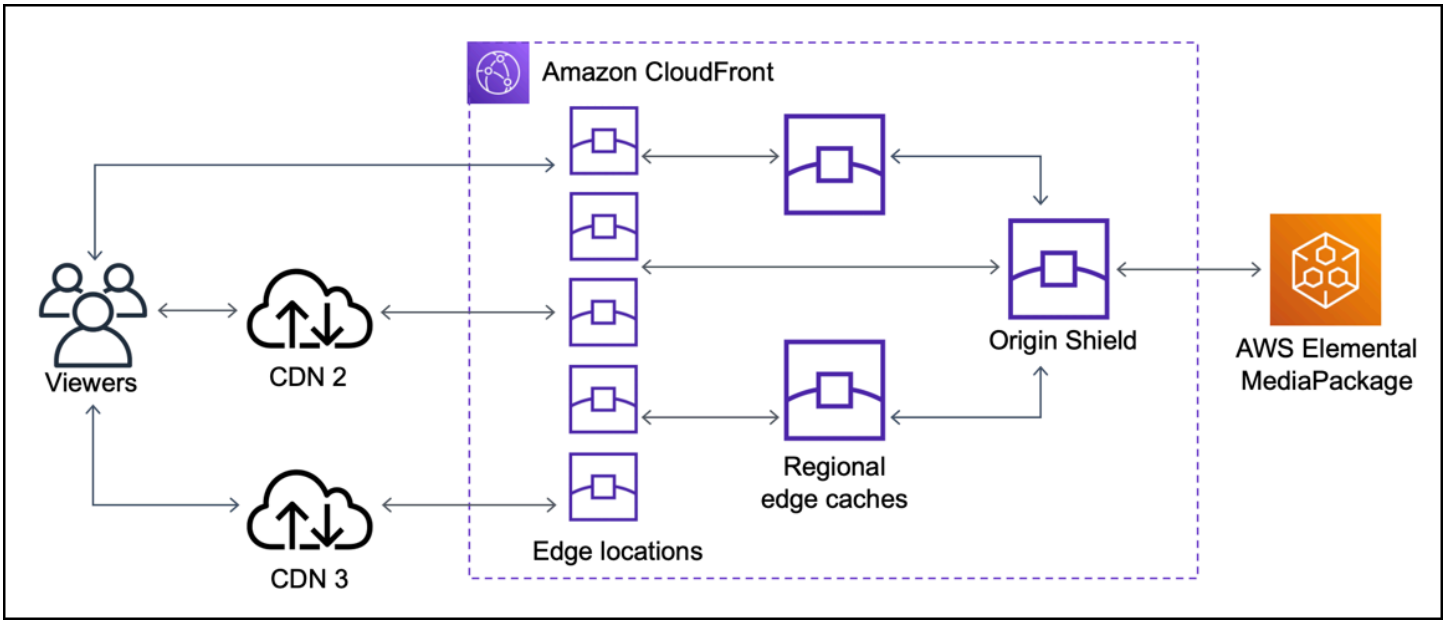
Sans Origin Shield (plusieurs réseaux de diffusion de contenu)

Sans Origin Shield, votre origine peut recevoir de nombreuses demandes en double pour le même contenu, chacune provenant d'un réseau de diffusion de contenu différent, comme indiqué dans le diagramme suivant.



Avec Origin Shield (plusieurs réseaux de diffusion de contenu)

L'utilisation d'Origin Shield, CloudFront comme origine pour vos autres CDN, peut contribuer à réduire la charge sur votre origine, comme le montre le schéma suivant.



Cliquez sur l'onglet AWS Région pour Origin Shield

Amazon CloudFront propose Origin Shield dans AWS les régions CloudFront disposant d'un cache périphérique régional. Lorsque vous activez Origin Shield, vous choisissez la AWS région pour Origin Shield. Vous devez choisir la région AWS dont la latence vers votre origine est la plus faible. Vous pouvez utiliser Origin Shield avec des origines situées dans une AWS région ou non AWS.

Pour les origines dans un AWS Région

Si votre origine se trouve dans une AWS région, déterminez d'abord si votre origine se trouve dans une région dans laquelle Origin CloudFront Shield est proposé. CloudFront propose Origin Shield dans les AWS régions suivantes.

- US East (Ohio) – `us-east-2`
- USA Est (Virginie du Nord) – `us-east-1`
- USA Ouest (Oregon) – `us-west-2`
- Asie-Pacifique (Mumbai) – `ap-south-1`
- Asie-Pacifique (Séoul) – `ap-northeast-2`
- Asie-Pacifique (Singapour) – `ap-southeast-1`
- Asie-Pacifique (Sydney) – `ap-southeast-2`
- Asie-Pacifique (Tokyo) : `ap-northeast-1`

- Europe (Francfort) – `eu-central-1`
- Europe (Irlande) – `eu-west-1`
- Europe (Londres) – `eu-west-2`
- Europe (Paris) : `eu-west-3`
- Amérique du Sud (São Paulo) – `sa-east-1`
- Moyen-Orient (Émirats arabes unis) — `me-central-1`

Si votre origine se trouve dans une AWS région CloudFront proposant Origin Shield

Si votre origine se trouve dans une AWS région qui CloudFront propose Origin Shield (voir la liste précédente), activez Origin Shield dans la même région que votre origine.

Si votre origine ne se trouve pas dans une AWS région CloudFront proposant Origin Shield

Si votre origine ne se trouve pas dans une AWS région CloudFront proposant Origin Shield, consultez le tableau suivant pour déterminer dans quelle région activer Origin Shield.

Si votre origine est dans...	Activer Origin Shield dans ...
US West (N. California) – `us-west-1`	US West (Oregon) – `us-west-2`
Africa (Cape Town) – `af-south-1`	Europe (Ireland) – `eu-west-1`
Asia Pacific (Hong Kong) – `ap-east-1`	Asia Pacific (Singapore) – `ap-southeast-1`
Canada (Central) – `ca-central-1`	US East (N. Virginia) – `us-east-1`
Europe (Milan) – `eu-south-1`	Europe (Frankfurt) – `eu-central-1`
Europe (Stockholm) – `eu-north-1`	Europe (London) – `eu-west-2`
Middle East (Bahrain) – `me-south-1`	Asia Pacific (Mumbai) – `ap-south-1`

Pour les origines situées en dehors de AWS

Vous pouvez utiliser Origin Shield avec une origine sur site ou ne se trouvant pas dans une région AWS . Dans ce cas, activez Origin Shield dans la AWS région où la latence par rapport à votre

origine est la plus faible. Si vous ne savez pas quelle AWS région présente la latence la plus faible par rapport à votre point d'origine, vous pouvez utiliser les suggestions suivantes pour vous aider à prendre une décision.

- Vous pouvez consulter le tableau précédent pour avoir une idée de la région AWS pouvant présenter la latence la plus faible vers votre origine, en fonction de l'emplacement géographique de votre origine.
- Vous pouvez lancer des instances Amazon EC2 dans différentes AWS régions géographiquement proches de votre origine et effectuer des tests `ping` pour mesurer les latences réseau typiques entre ces régions et votre origine.

Activer Origin Shield

Vous pouvez activer Origin Shield pour améliorer votre taux d'accès au cache, réduire la charge sur votre origine et améliorer les performances. Pour activer Origin Shield, modifiez les paramètres d'origine dans une CloudFront distribution. Origin Shield est une propriété de l'origine. Pour chaque origine de vos CloudFront distributions, vous pouvez activer Origin Shield séparément dans AWS la région offrant les meilleures performances pour cette origine.

Vous pouvez activer Origin Shield dans la CloudFront console CloudFormation, avec ou avec l' CloudFrontAPI.

Console

Pour activer Origin Shield pour une origine existante (console)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution contenant l'origine à mettre à jour.
3. Choisissez l’onglet Origines.
4. Choisissez l'origine à mettre à jour, puis choisissez Edit (Modifier).
5. Pour Enable Origin Shield (Activer Origin Shield), choisissez Yes (Oui).
6. Pour Origin Shield Region (Région pour Origin Shield), choisissez la région AWS dans laquelle vous souhaitez activer Origin Shield. Pour obtenir de l’aide sur le choix d’une région, consultez Cliquez sur l'onglet AWS Région pour Origin Shield.
7. Cliquez sur Enregistrer les modifications.

Lorsque le statut de votre distribution est Déployée, Origin Shield est prêt. Cela prend quelques minutes.

Pour activer Origin Shield pour une nouvelle origine (console)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Pour créer la nouvelle origine dans une distribution existante, procédez comme suit :

   1. Choisissez la distribution dans laquelle vous souhaitez créer l'origine.
   2. Choisissez Créer une origine, puis passez à l'étape 3.

   Pour créer la nouvelle origine dans une nouvelle distribution standard, procédez comme suit :

   1. Suivez ces étapes pour créer une distribution standard dans la console. Pour plus d'informations, consultez Création d'une CloudFront distribution dans la console.
   2. Dans la section Paramètres, sélectionnez Personnaliser les paramètres d'origine. Passez à l'étape 3.
3. Pour Activer Origin Shield, choisissez Oui.
4. Pour Origin Shield Region (Région pour Origin Shield), choisissez la région AWS dans laquelle vous souhaitez activer Origin Shield. Pour obtenir de l'aide sur le choix d'une région, consultez Cliquez sur l'onglet AWS Région pour Origin Shield.
5. Suivez les étapes de la console pour terminer la création de votre origine ou de votre distribution.

Lorsque le statut de votre distribution est Déployée, Origin Shield est prêt. Cela prend quelques minutes.

CloudFormation

Pour activer Origin Shield avec CloudFormation, utilisez la `OriginShield` propriété dans le type de `Origin` propriété d'une `AWS::CloudFront::Distribution` ressource. Vous pouvez ajouter la propriété `OriginShield` à un type de propriété `Origin` existant, ou l'inclure lorsque vous créez un nouveau type de propriété `Origin`.

L'exemple suivant présente la syntaxe, au format YAML, pour l'activation d'`OriginShield` dans la région USA Ouest (Oregon) (`us-west-2`). Pour obtenir de l'aide sur le choix d'une région, consultez the section called "Cliquez sur l'onglet AWS Région pour Origin Shield". Cet

exemple montre uniquement le type de propriété `Origin`, et non l'ensemble de la ressource `AWS::CloudFront::Distribution`.

```
Origins:
- DomainName: 3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com
  Id: Example-EMP-3ae97e9482b0d011
  OriginShield:
    Enabled: true
    OriginShieldRegion: us-west-2
  CustomOriginConfig:
    OriginProtocolPolicy: match-viewer
    OriginSSLProtocols: TLSv1
```

Pour plus d'informations, voir AWS::CloudFront::Distribution Origin dans la section de référence des ressources et des propriétés du Guide de l'AWS CloudFormation utilisateur.

API

Pour activer Origin Shield avec l' CloudFront API à l'aide AWS des SDK ou AWS Command Line Interface (AWS CLI), utilisez le `OriginShield` type. Vous spécifiez `OriginShield` dans un type `Origin`, dans un type`DistributionConfig`. Pour plus d'informations sur le `OriginShield` type, consultez les informations suivantes dans le Amazon CloudFront API Reference.

- OriginShield(type)
- Origin (type)
- DistributionConfig(type)
- UpdateDistribution(opération)
- CreateDistribution(opération)

La syntaxe spécifique pour l'utilisation de ces types et opérations varie en fonction du client SDK, CLI ou de l'API. Pour plus d’informations, consultez la documentation de référence de votre kit SDK, CLI ou client.

Estimation des frais liés à Origin Shield

Les frais liés à Origin Shield augmentent en fonction du nombre de demandes adressées à Origin Shield en tant que couche incrémentielle.

Pour les demandes dynamiques (ne pouvant pas être mises en cache) qui sont transmises par proxy à l'origine, Origin Shield est toujours une couche incrémentielle. Les demandes dynamiques utilisent les méthodes HTTP `PUT`, `POST`, `PATCH` et `DELETE`.

Les demandes `GET` et `HEAD` dont la durée de vie est inférieure à 3 600 secondes sont considérées comme des demandes dynamiques. En outre, les demandes `GET` et `HEAD` dont la mise en cache est désactivée sont également considérées comme des demandes dynamiques.

Pour estimer vos frais liés à Origin Shield pour les demandes dynamiques, utilisez la formule suivante :

Nombre total de demandes dynamiques x frais Origin Shield pour 10 000 demandes / 10 000

Pour les demandes non dynamiques utilisant les méthodes HTTP `GET`, `HEAD` et `OPTIONS`, Origin Shield constitue parfois une couche supplémentaire. Lorsque vous activez Origin Shield, vous choisissez Origin Shield. Région AWS Pour les demandes qui sont naturellement dirigées vers le cache périphérique régional de la même région qu'Origin Shield, Origin Shield sera ignoré. Vous n’avez pas de frais Origin Shield supplémentaires pour ces demandes. Pour les demandes qui vont vers un cache périphérique régional dans une autre région que celle d’Origin Shield, puis vers Origin Shield, Origin Shield est une couche incrémentielle. Des frais Origin Shield supplémentaires seront facturés pour ces demandes.

Pour estimer vos frais liés à Origin Shield pour les demandes pouvant être mises en cache, utilisez la formule suivante :

Nombre total de demandes pouvant être mises en cache x (1 – taux d'accès au cache) x pourcentage de demandes allant à Origin Shield à partir d'un cache périphérique régional dans une autre région x frais Origin Shield pour 10 000 demandes / 10 000

Pour de plus amples informations sur les frais liés à 10 000 demandes pour Origin Shield, veuillez consulter Tarification CloudFront .

Haute disponibilité d'Origin Shield

Origin Shield tire parti de la fonctionnalité de caches périphériques CloudFront régionaux. Chacun de ces caches périphériques est créé dans une AWS région utilisant au moins trois zones de disponibilité avec des flottes d'instances Amazon EC2 auto-scalables. Les connexions à Origin Shield à partir d'emplacements CloudFront utilisent également le suivi actif d'erreurs pour chaque demande, afin d'acheminer automatiquement la demande vers un emplacement Origin Shield secondaire si l'emplacement Origin Shield principal n'est pas disponible.

Comment Origin Shield interagit avec les autres fonctionnalités CloudFront

Les sections suivantes expliquent comment Origin Shield interagit avec d'autres fonctions CloudFront.

Origin Shield et CloudFront journalisation

Pour connaître le moment où Origin Shield a traité une demande, vous devez activer l'une des options suivantes :

- CloudFront journaux standard (journaux d'accès). Les journaux standard sont fournis gratuitement.
- CloudFront journaux d'accès en temps réel. L'utilisation des journaux d'accès en temps réel entraîne des frais supplémentaires. Consultez les CloudFronttarifs d'Amazon.

Les accès au cache provenant d'Origin Shield apparaissent comme `OriginShieldHit` `x-edge-detailed-result-type` sur le terrain dans CloudFront les journaux. Origin Shield exploite les caches périphériques CloudFront régionaux d'Amazon. Si une demande est acheminée depuis un emplacement CloudFront périphérique vers le cache périphérique régional qui agit en tant qu'Origin Shield, elle est signalée comme un `Hit` dans les journaux, et non comme un`OriginShieldHit`.

Origin Shield et groupes d'origines

Origin Shield est compatible avec les groupes d'origines CloudFront . Origin Shield étant une propriété de l'origine, les demandes passent toujours par Origin Shield pour chaque origine, même lorsque l'origine fait partie d'un groupe d'origines. Pour une demande donnée, CloudFront achemine la demande vers l'origine principale du groupe d'origine via le Origin Shield de l'origine principale. Si cette demande échoue (selon les critères de basculement du groupe d'origine), CloudFront achemine la demande vers l'origine secondaire via le Origin Shield de l'origine secondaire.

Origin Shield et Lambda@Edge

Origin Shield n'a pas d'impact sur l'exécution des fonctions de Lambda@Edge, mais peut affecter la région AWS dans laquelle ces fonctions s'exécutent.

Lorsque vous utilisez Origin Shield avec Lambda @Edge, les déclencheurs orientés vers l'origine (demande d'origine et réponse d'origine) s'exécutent dans la région AWS où Origin Shield est activé. Si l'emplacement Origin Shield principal n'est pas disponible et CloudFront achemine les demandes vers un emplacement Origin Shield secondaire, les déclencheurs Lambda @Edge orientés vers l'origine seront également déplacés pour utiliser l'emplacement secondaire d'Origin Shield.

Viewer-facing les déclencheurs ne sont pas affectés.

Optimisez la haute disponibilité grâce au basculement CloudFront d'origine

Vous pouvez configurer le CloudFront basculement d'origine pour les scénarios nécessitant une haute disponibilité. Pour commencer, vous créez un groupe d'origine avec deux origines : une principale et une secondaire. Si l'origine principale n'est pas disponible ou renvoie des codes d'état de réponse HTTP spécifiques indiquant un échec, bascule CloudFront automatiquement vers l'origine secondaire.

Pour configurer le basculement d'origine, vous devez avoir une distribution avec au moins deux origines. Ensuite, vous créez un groupe d'origine pour votre distribution incluant deux origines, en en définissant une comme la principale. Enfin, vous créez ou mettez à jour un comportement de cache pour utiliser le groupe d'origine.

Pour voir les étapes de configuration des groupes d’origine et des options de basculement pour une origine spécifique, consultez Création d’un groupe d’origine.

Après avoir configuré le basculement à l'origine pour un comportement de cache, effectuez les CloudFront opérations suivantes pour les requêtes des spectateurs :

- En cas d'accès au cache, CloudFront renvoie l'objet demandé.
- En cas d'échec du cache, CloudFront achemine la demande vers l'origine principale du groupe d'origine.
- Lorsque l'origine principale renvoie un code d'état qui n'est pas configuré pour le basculement, tel qu'un code d'état HTTP 2xx ou 3xx, elle transmet l'objet CloudFront demandé au visualiseur.
- Lorsque l'une des situations suivantes se produit :
  - L'origine principale renvoie un code d'état HTTP que vous avez configuré pour le basculement
  - CloudFront ne parvient pas à se connecter à l'origine principale (lorsque 503 est défini comme code de basculement)
  - La réponse de l’origine principale dépasse le délai d’attente (délai dépassé) (lorsque le code 504 est défini comme code de basculement)

  CloudFront Achemine ensuite la demande vers l'origine secondaire du groupe d'origine.

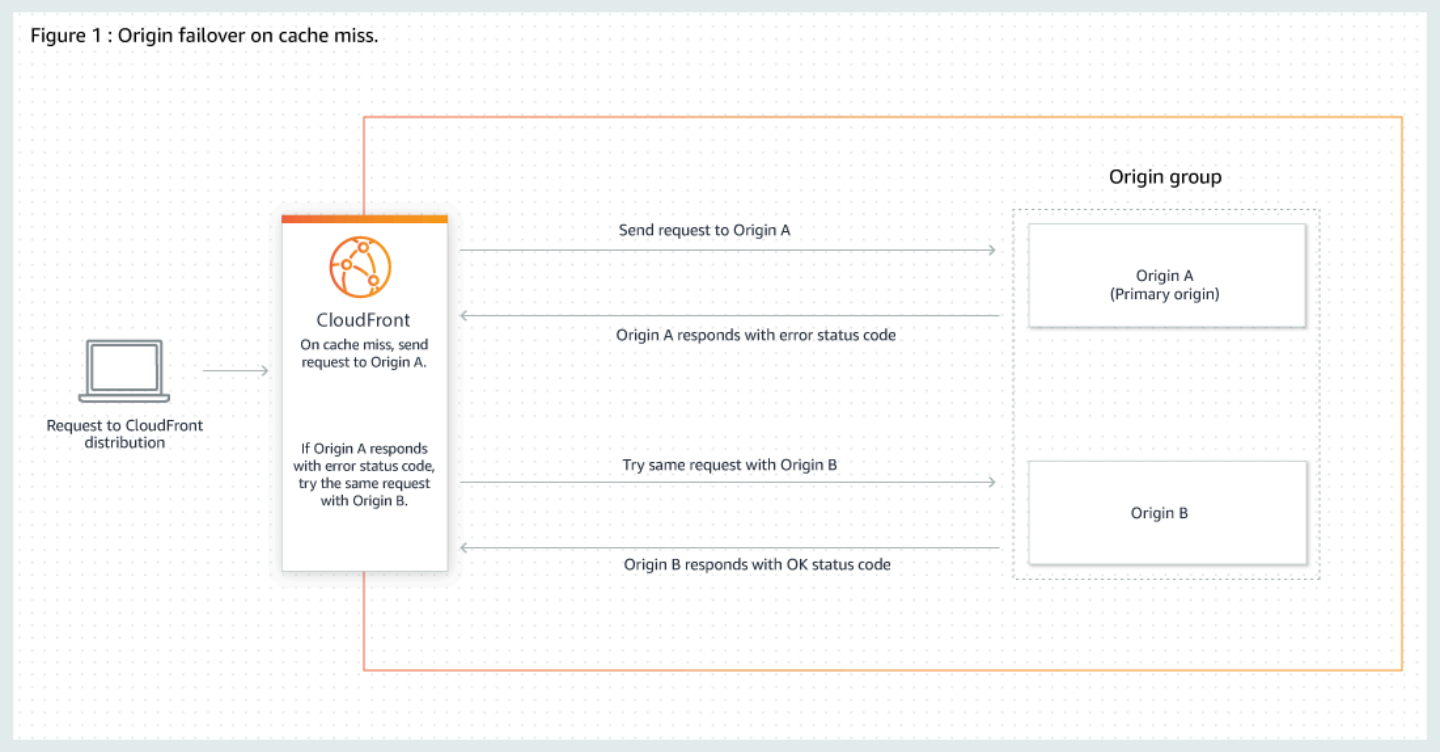
> **Note**
>
> Dans certains cas d'utilisation, tels que le streaming de contenu vidéo, vous CloudFront souhaiterez peut-être basculer rapidement vers l'origine secondaire. Pour ajuster la rapidité CloudFront du basculement vers l'origine secondaire, consultezContrôle des délais d'expiration et des tentatives de l'origine.

CloudFront achemine toutes les demandes entrantes vers l'origine principale, même lorsqu'une demande précédente a échoué vers l'origine secondaire. CloudFront envoie des demandes à l'origine secondaire uniquement en cas d'échec d'une demande à l'origine principale.

CloudFront bascule vers l'origine secondaire uniquement lorsque la méthode HTTP de la demande du visualiseur est `GET`, `HEAD`, ou`OPTIONS`. CloudFront ne bascule pas lorsque l'utilisateur envoie une méthode HTTP différente (par exemple `POST`, `PUT`, et ainsi de suite).

> **Note**
>
> CloudFront ne basculera pas si ce paramètre `OPTIONS` n'est pas défini Méthodes HTTP mises en cache dans le comportement de votre cache.

Le graphique suivant illustre le fonctionnement du basculement d'origine



Rubriques

- Création d’un groupe d’origine
- Contrôle des délais d’expiration et des tentatives de l’origine
- Utilisation du basculement d'origine avec les fonctions Lambda@Edge
- Utilisation des pages d'erreur personnalisées avec le basculement d'origine

Création d’un groupe d’origine

Pour créer un groupe d'origine

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution pour laquelle vous souhaitez créer le groupe d'origine.
3. Choisissez l’onglet Origines.
4. Assurez-vous qu’il existe plusieurs origines pour la distribution. Si ce n'est pas le cas, ajoutez une deuxième origine.
5. Sous l'onglet Origins (Origines) du volet Origin groups (Groupes d'origines), choisissez Create origin group (Créer un groupe d'origines).

6. Choisissez les origines du groupe d'origine. Après avoir ajouté des origines, utilisez les flèches pour définir la priorité, c'est-à-dire l'origine principale et l'origine secondaire.
7. Saisissez un nom pour le groupe d’origines.
8. Choisissez les codes d'état HTTP à utiliser comme critères de basculement. Vous pouvez choisir n'importe quelle combinaison des codes d'état suivants : 400, 403, 404, 416, 429, 500, 502, 503 ou 504. Lorsque CloudFront reçoit une réponse contenant l'un des codes d'état que vous avez spécifiés, elle bascule vers l'origine secondaire.

   > **Note**
   >
   > CloudFront bascule vers l'origine secondaire uniquement lorsque la méthode HTTP de la demande du visualiseur est `GET`, `HEAD`, ou `OPTIONS`. CloudFront ne bascule pas lorsque l'utilisateur envoie une méthode HTTP différente (par exemple `POST`, `PUT`, et ainsi de suite).

9. Dans Critères de sélection des origines, indiquez comment vos origines sont sélectionnées lorsque votre distribution achemine les demandes des utilisateurs. Vous pouvez choisir les options suivantes.

   Par défaut

   CloudFront utilisera la priorité d'origine par défaut que vous spécifiez sur la page Paramètres.

   Score de qualité des médias

   CloudFront suit et utilise ce score pour déterminer la première origine à laquelle transmettre la demande. Cela autorise également CloudFront à envoyer des `HEAD` requêtes asynchrones à l'origine alternative du groupe d'origine afin de déterminer son score de qualité multimédia. Vous ne pouvez choisir cette option que pour les origines de la AWS Elemental MediaPackage v2. Pour plus d’informations, consultez Résilience tenant compte de la qualité média.

10. Choisissez Create origin group (Créer un groupe d'origines).

Assurez-vous de définir votre groupe d’origines comme origine pour le comportement de cache de votre distribution. Pour plus d’informations, consultez Nom.

Contrôle des délais d’expiration et des tentatives de l’origine

Par défaut, CloudFront essaie de se connecter à l'origine principale d'un groupe d'origine pendant 30 secondes (3 tentatives de connexion de 10 secondes chacune) avant de basculer vers l'origine secondaire. Dans certains cas d'utilisation, tels que le streaming de contenu vidéo, vous CloudFront souhaiterez peut-être basculer plus rapidement vers l'origine secondaire. Vous pouvez ajuster les paramètres suivants pour modifier la rapidité du CloudFront basculement vers l'origine secondaire. Si l'origine est une origine secondaire ou une origine qui ne fait pas partie d'un groupe d'origine, ces paramètres influent sur la rapidité CloudFront avec laquelle une réponse HTTP 504 est renvoyée à l'utilisateur.

Pour basculer plus rapidement, spécifiez un délai d'expiration de connexion plus court, moins de tentatives de connexion, ou les deux. Pour les origines personnalisées (y compris les origines de compartiment Amazon S3 qui sont configurées avec un hébergement de site web statique), vous pouvez également ajuster le délai d'expiration de la réponse d'origine.

Délai d'expiration de la connexion d'origine

: Le paramètre de délai d'expiration de la connexion à l'origine affecte la durée d' CloudFront attente lors de la tentative d'établissement d'une connexion avec l'origine. Par défaut, le CloudFront délai d'attente est de 10 secondes pour établir une connexion, mais vous pouvez spécifier 1 à 10 secondes (inclus). Pour plus d’informations, consultez Délai de connexion.

Tentatives de connexion de l'origine

: Le paramètre Tentatives de connexion à l'origine affecte le nombre de CloudFront tentatives de connexion à l'origine. Par défaut, CloudFront essaie de se connecter 3 fois, mais vous pouvez spécifier 1 à 3 (inclus). Pour plus d’informations, consultez Tentatives de connexion.

  Pour une origine personnalisée (y compris un compartiment Amazon S3 configuré avec un hébergement de site Web statique), ce paramètre affecte également le nombre de CloudFront tentatives d'obtention d'une réponse de la part de l'origine en cas d'expiration d'un délai de réponse d'origine.

Délai de réponse de l’origine

: Le délai de réponse de l'origine, également appelé délai de lecture de l'origine, affecte le temps d' CloudFront attente avant de recevoir une réponse (ou de recevoir la réponse complète) de l'origine. Par défaut, le CloudFront délai d'attente est de 30 secondes, mais vous pouvez spécifier 1 à 120 secondes (inclus). Pour plus d’informations, consultez Délai de réponse.

Comment modifier ces paramètres

Pour modifier ces paramètres dans la console CloudFront

- Pour une nouvelle origine ou une nouvelle distribution, vous spécifiez ces valeurs lorsque vous créez la ressource.
- Pour une origine existante dans une distribution existante, vous spécifiez ces valeurs lorsque vous modifiez l'origine.

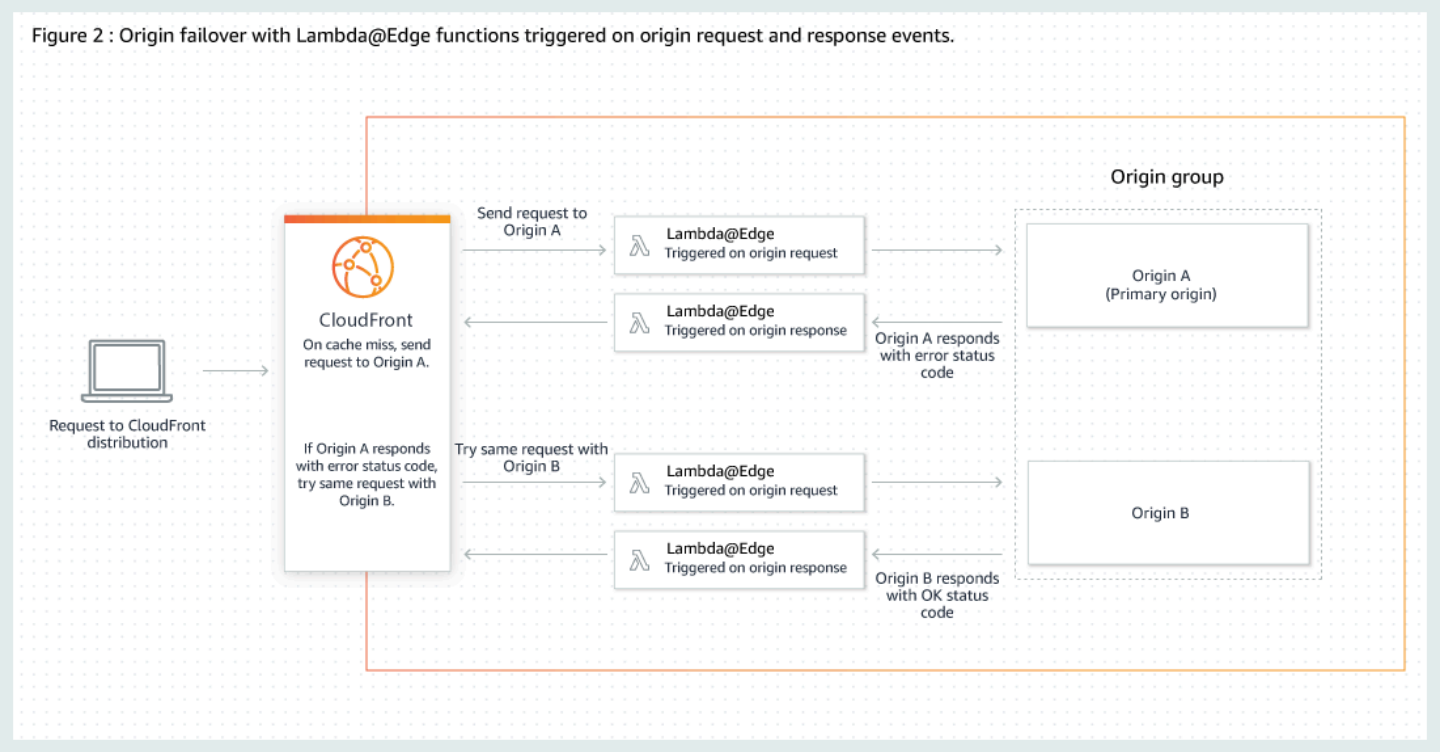
Pour plus d’informations, consultez Référence de tous les paramètres de distribution.

Utilisation du basculement d'origine avec les fonctions Lambda@Edge

Vous pouvez utiliser les fonctions Lambda @Edge avec des CloudFront distributions que vous avez configurées avec des groupes d'origine. Pour utiliser une fonction Lambda, spécifiez-la dans une demande d'origine ou un déclencheur de réponse de l'origine pour un groupe d'origine lorsque vous créez le comportement de cache. Lorsque vous utilisez une fonction Lambda@Edge avec un groupe d'origine, la fonction peut être déclenchée deux fois pour une seule demande d'utilisateur. Par exemple, envisagez le scénario suivant :

1. Vous créez une fonction Lambda@Edge avec un déclencheur de demande d'origine.
2. La fonction Lambda est déclenchée une fois lors de l' CloudFront envoi d'une requête à l'origine principale (en cas d'échec du cache).
3. L'origine principale répond avec un code d'état HTTP configuré pour le basculement.
4. La fonction Lambda est à nouveau déclenchée lors de l' CloudFront envoi de la même requête à l'origine secondaire.

Le schéma suivant illustre la façon dont le basculement d'origine fonctionne lorsque vous incluez une fonction Lambda@Edge dans une requête d'origine ou un déclencheur de réponse.



Pour plus d'informations sur l'utilisation des déclencheurs Lambda@Edge, consultez the section called “Ajout de déclencheurs pour une fonction Lambda@Edge”.

Pour plus d’informations sur la gestion du basculement DNS, consultez Configuration du basculement DNS dans le Guide du développeur Amazon Route 53.

Utilisation des pages d'erreur personnalisées avec le basculement d'origine

Vous pouvez utiliser des pages d'erreur personnalisées avec des groupes d'origine de la même façon dont vous les utiliseriez avec des origines qui ne sont pas configurées pour le basculement d'origine.

Lorsque vous utilisez le basculement d'origine, vous pouvez configurer CloudFront pour renvoyer une page d'erreur personnalisée pour l'origine principale ou secondaire (ou les deux) :

- Renvoie une page d'erreur personnalisée pour l'origine principale : si l'origine principale renvoie un code d'état HTTP qui n'est pas configuré pour le basculement, CloudFront renvoie la page d'erreur personnalisée aux utilisateurs.
- Renvoie une page d'erreur personnalisée pour l'origine secondaire : si l'origine secondaire CloudFront reçoit un code d'état d'échec, CloudFront renvoie la page d'erreur personnalisée.

Pour plus d'informations sur l'utilisation de pages d'erreur personnalisées avec CloudFront, consultezGénération de réponses aux·erreurs personnalisées.

Gestion de la durée de conservation de contenu dans le cache (expiration)

Vous pouvez contrôler la durée pendant laquelle vos fichiers restent en CloudFront cache avant de CloudFront transmettre une autre demande à votre source. En réduisant la durée, vous pouvez diffuser du contenu dynamique. Augmenter la durée signifie que vos utilisateurs obtiennent de meilleures performances parce que vos fichiers sont plus susceptibles d'être servis directement à partir du cache périphérique. Une durée plus longue réduit également la charge sur votre origine.

Généralement, CloudFront diffuse un fichier depuis un emplacement périphérique jusqu'à ce que la durée de cache que vous avez spécifiée soit écoulée, c'est-à-dire jusqu'à ce que le fichier expire. Après son expiration, la prochaine fois que l'emplacement périphérique reçoit une demande pour le fichier, il CloudFront transmet la demande à l'origine pour vérifier que le cache contient la dernière version du fichier. La réponse de l'origine varie selon que le fichier a changé ou non :

- Si le CloudFront cache possède déjà la dernière version, l'origine renvoie un code d'état`304 Not Modified`.
- Si le CloudFront cache ne possède pas la dernière version, l'origine renvoie un code d'état `200 OK` et la dernière version du fichier.

Si un fichier situé dans un emplacement périphérique n'est pas fréquemment demandé, vous CloudFront pouvez l'expulser (supprimer le fichier avant sa date d'expiration) pour faire de la place pour les fichiers qui ont été demandés plus récemment.

Nous vous recommandons de gérer la durée de votre cache en mettant à jour la politique de cache de votre distribution. Si vous choisissez de ne pas utiliser de politique de cache, la durée de vie par défaut est de 24 heures, mais vous pouvez mettre à jour les paramètres suivants pour remplacer cette valeur par défaut :

- Pour modifier la durée du cache pour tous les fichiers qui correspondent au même modèle de chemin, vous pouvez modifier CloudFront les paramètres du TTL minimum, du TTL maximum et du TTL par défaut pour le comportement du cache. Pour en savoir plus sur les paramètres individuels, consultez Durée de vie minimale, Durée de vie (TTL) maximale et TTL par défaut.

- Pour changer la durée de conservation en cache pour un fichier individuel, vous pouvez configurer votre origine de sorte à ajouter un en-tête `Cache-Control` avec la directive `max-age` ou `s-maxage`, ou un en-tête `Expires` au fichier. Pour plus d'informations, consultez Utilisation des en-têtes pour contrôler la durée de conservation en cache pour des objets individuels.

Pour plus d'informations sur la manière dont la durée de vie minimale, la durée de vie par défaut et la durée de vie maximale interagissent avec les directives `max-age` et `s-maxage`, ainsi que le champ d'en-tête `Expires`, consultez the section called "Spécifiez la durée pendant laquelle les objets sont CloudFront mis en cache".

Vous pouvez également contrôler la durée pendant laquelle les erreurs (par exemple`404 Not Found`) restent dans le CloudFront cache avant de CloudFront réessayer d'obtenir l'objet demandé en transférant une autre demande vers votre origine. Pour plus d'informations, consultez the section called "Comment CloudFront traite les codes d'état HTTP 4xx et 5xx depuis votre origine".

Rubriques

- Utilisation des en-têtes pour contrôler la durée de conservation en cache pour des objets individuels
- Diffusion de contenu obsolète (expiré)
- Spécifiez la durée pendant laquelle les objets sont CloudFront mis en cache
- Ajout d'en-têtes à vos objets à l'aide de la console Amazon S3

Utilisation des en-têtes pour contrôler la durée de conservation en cache pour des objets individuels

Vous pouvez utiliser les en-têtes `Cache-Control` et `Expires` pour contrôler pendant combien de temps des objets restent dans le cache. Les valeurs de Durée de vie minimale, Durée de vie par défaut et Durée de vie maximale affectent également la durée de conservation en cache, mais voici un aperçu de l'incidence de ces en-têtes sur cette durée :

- Grâce à `Cache-Control max-age` cette directive, vous pouvez spécifier la durée (en secondes) pendant laquelle vous souhaitez qu'un objet reste dans le cache avant de CloudFront le récupérer à nouveau depuis le serveur d'origine. Le délai d'expiration minimum pris CloudFront en charge est de 0 seconde. La valeur maximale est 100 ans. Spécifiez la valeur au format suivant :

  ```
  Cache-Control: max-age=seconds
  ```

Par exemple, la directive suivante indique CloudFront de conserver l'objet associé dans le cache pendant 3 600 secondes (une heure) :

```
Cache-Control: max-age=3600
```

Si vous souhaitez que les objets restent dans CloudFront les caches périphériques pendant une durée différente de celle dans les caches du navigateur, vous pouvez utiliser les `Cache-Control s-maxage` directives `Cache-Control max-age` et conjointement. Pour plus d'informations, consultez Spécifiez la durée pendant laquelle les objets sont CloudFront mis en cache.

- Le champ d'`Expires`en-tête vous permet de spécifier une date et une heure d'expiration en utilisant le format spécifié dans la RFC 2616, Protocole de transfert hypertexte -- HTTP/1.1 Section 3.3.1, Date complète, par exemple :

  ```
  Sat, 27 Jun 2015 23:59:59 GMT
  ```

Nous vous recommandons d'utiliser la directive `Cache-Control max-age` plutôt que le champ d'en-tête `Expires` pour contrôler la mise en cache des objets. Si vous spécifiez des valeurs pour `Cache-Control max-age` et pour `Expires`, CloudFront utilise uniquement la valeur de `Cache-Control max-age`.

Pour plus d'informations, consultez Spécifiez la durée pendant laquelle les objets sont CloudFront mis en cache.

Vous ne pouvez pas utiliser les champs HTTP `Cache-Control` ou d'`Pragma`en-tête dans une `GET` requête émanant d'un utilisateur CloudFront pour forcer le retour au serveur d'origine de l'objet. CloudFront ignore ces champs d'en-tête dans les requêtes des spectateurs.

Pour plus d'informations sur les champs `Expires` d'en-tête `Cache-Control` et, consultez les sections suivantes de la RFC 2616, Hypertext Transfer Protocol -- : HTTP/1.1

- Section 14.9 Cache Control
- Section 14.21 Expires

Diffusion de contenu obsolète (expiré)

CloudFront prend en charge `Stale-While-Revalidate` les directives de contrôle du `Stale-If-Error` cache et. Vous pouvez utiliser ces directives pour définir la durée pendant laquelle le contenu obsolète reste accessible aux utilisateurs.

Rubriques

- Stale-While-Revalidate
- Stale-If-Error
- Utilisation des deux directives

`Stale-While-Revalidate`

Cette directive permet CloudFront de diffuser du contenu obsolète depuis le cache tout en récupérant de CloudFront manière asynchrone une nouvelle version depuis l'origine. Cela permet d'améliorer la latence, car les utilisateurs reçoivent immédiatement les réponses depuis les emplacements périphériques sans devoir attendre la récupération en arrière-plan. Le nouveau contenu est chargé en arrière-plan pour les prochaines demandes.

Example Exemple : **`Stale-While-Revalidate`**

CloudFront effectue les opérations suivantes lorsque vous définissez l'`Cache-Control`en-tête pour utiliser ces directives.

```
Cache-Control: max-age=3600, stale-while-revalidate=600
```

1. CloudFront mettra en cache une réponse pendant une heure (`max-age=3600`).
2. Si une demande est faite après cette durée, CloudFront sert le contenu obsolète, tout en envoyant simultanément une demande à l'origine pour revalider et actualiser le contenu mis en cache.
3. Pendant la revalidation du contenu, CloudFront diffuse le contenu obsolète pendant 10 minutes ()`stale-while-revalidate=600`.

> **Note**
>
> CloudFront diffusera le contenu obsolète jusqu'à la valeur de la `stale-while-revalidate` directive ou à la valeur du TTL CloudFront maximum, la valeur la plus faible étant retenue.

Une fois la durée de vie maximale écoulée, l'objet obsolète n'est plus disponible dans le cache périphérique, quelle que soit sa valeur `stale-while-revalidate`.

`Stale-If-Error`

Cette directive permet CloudFront de diffuser du contenu obsolète depuis le cache si l'origine est inaccessible ou renvoie un code d'erreur compris entre 500 et 600. Cela garantit que les spectateurs peuvent accéder au contenu même pendant une panne d'origine.

Example Exemple : **`Stale-If-Error`**

CloudFront effectue les opérations suivantes lorsque vous définissez l'`Cache-Control`en-tête pour utiliser ces directives.

```
Cache-Control: max-age=3600, stale-if-error=86400
```

1. CloudFront met la réponse en cache pendant une heure (`max-age=3600`).
2. Si l'origine est en panne ou renvoie une erreur après cette durée, CloudFront continue de diffuser le contenu obsolète pendant 24 heures maximum () `stale-if-error=86400`
3. Si vous avez configuré des réponses d'erreur personnalisées, CloudFront tentera de diffuser le contenu obsolète si une erreur est détectée pendant la `stale-if-error` durée spécifiée. Si le contenu obsolète n'est pas disponible, les réponses d'erreur personnalisées que vous avez configurées pour le code d'état d'erreur correspondant CloudFront seront alors diffusées. Pour plus d'informations, consultez Génération de réponses aux·erreurs personnalisées.

Remarques

- CloudFront diffusera le contenu obsolète jusqu'à la valeur de la `stale-if-error` directive ou à la valeur du TTL CloudFront maximum, la valeur la plus faible étant retenue. Une fois la durée de vie maximale écoulée, l'objet obsolète n'est plus disponible dans le cache périphérique, quelle que soit sa valeur `stale-if-error`.
- Si vous ne configurez pas `stale-if-error` ou ne personnalisez pas les réponses aux erreurs, vous CloudFront renverrez l'objet obsolète ou la transmettrez au visualiseur, selon que l'objet demandé se trouve ou non dans le cache périphérique. Pour plus

d'informations, consultez Comment traiter CloudFront les erreurs si vous n'avez pas configuré de pages d'erreur personnalisées.

Utilisation des deux directives

`stale-while-revalidate` et `stale-if-error` sont des directives de contrôle du cache indépendantes que vous pouvez utiliser ensemble pour réduire la latence et ajouter une mémoire tampon permettant à votre origine de répondre ou de récupérer.

Example Exemple : utilisation des deux directives

CloudFront effectue les opérations suivantes lorsque vous définissez l'`Cache-Control`en-tête pour utiliser les directives suivantes.

```
Cache-Control: max-age=3600, stale-while-revalidate=600, stale-if-error=86400
```

1. CloudFront met la réponse en cache pendant une heure (`max-age=3600`).
2. Si une demande est faite après cette durée, CloudFront diffuse le contenu obsolète pendant 10 minutes maximum (`stale-while-revalidate=600`) pendant la revalidation du contenu.
3. Si le serveur d'origine renvoie une erreur alors qu'il CloudFront tente de revalider le contenu, CloudFront il continuera à diffuser le contenu obsolète pendant 24 heures au maximum ()`stale-if-error=86400`.

La mise en cache est un équilibre entre performance et actualisation. L'utilisation de directives telles que `stale-while-revalidate` et `stale-if-error` peut améliorer les performances et l'expérience utilisateur, mais vérifiez que les configurations correspondent à l'actualisation souhaitée pour votre contenu. Les directives de contenu obsolètes conviennent mieux aux cas d'utilisation où le contenu doit être actualisé, mais où il n'est pas essentiel de disposer de la dernière version. De plus, si votre contenu ne change pas ou change rarement, `stale-while-revalidate` peut ajouter des demandes réseau inutiles. Envisagez plutôt de définir une durée de cache longue.

Spécifiez la durée pendant laquelle les objets sont CloudFront mis en cache

Pour contrôler la durée pendant laquelle un objet CloudFront est conservé dans le cache avant d'envoyer une autre demande à l'origine, vous pouvez :

- Définissez les valeurs TTL minimale, maximale et par défaut dans le comportement du cache d'une CloudFront distribution. Vous pouvez définir ces valeurs dans une politique de cache associée au comportement de cache (recommandé) ou dans les paramètres de cache hérités.
- inclure l'en-tête `Cache-Control` ou `Expires` dans les réponses de l'origine. Ces en-têtes permettent également de déterminer combien de temps un navigateur conserve un objet dans le cache du navigateur avant d'envoyer une autre demande à CloudFront.

Le tableau suivant explique comment les en-têtes `Cache-Control` et `Expires` envoyés à partir de l'origine fonctionnent avec les paramètres TTL dans un comportement de cache pour affecter la mise en cache.

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
L'origine ajoute une directive **`Cache-Control: max-age`** à l'objet	CloudFront mise en cache CloudFront met l'objet en cache pour la valeur la plus faible entre la valeur de la `Cache-Control: max-age` directive ou la valeur du TTL CloudFront maximum. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la directive `Cache-Control: max-age`.	CloudFront mise en cache CloudFront la mise en cache dépend des valeurs du TTL CloudFront minimum et du TTL maximum et de la directive : `Cache-Control max-age` • Si TTL minimum < `max-age` < TTL maximum, l'objet est mis en CloudFront cache pour la valeur de la directive . `Cache-Control: max-age` • Si `max-age` < TTL minimum, CloudFront met l'objet en cache pour la valeur du TTL CloudFront minimum. •

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
		Si `max-age` > TTL maximum, CloudFront met l'objet en cache pour la valeur du TTL CloudFront maximum. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la directive `Cache-Control: max-age`.
L'origine n'ajoute pas de directive **`Cache-Control: max-age`** à l'objet	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur du TTL CloudFront par défaut. Conservation en cache par les navigateurs Dépend du navigateur.	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur la plus élevée entre le TTL CloudFront minimum ou le TTL par défaut. Conservation en cache par les navigateurs Dépend du navigateur.

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
L'origine ajoute les directives **`Cache-Control: max-age`** et **`Cache-Control: s-maxage`** à l'objet	CloudFront mise en cache CloudFront met l'objet en cache pour la valeur la plus faible entre la valeur de la `Cache-Control: s-maxage` directive ou la valeur du TTL CloudFront maximum. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la directive `Cache-Control max-age`.	CloudFront mise en cache CloudFront la mise en cache dépend des valeurs du TTL CloudFront minimum et du TTL maximum et de la directive : `Cache-Control: s-maxage` • Si TTL minimum < `s-maxage` < TTL maximum, l'objet est mis en CloudFront cache pour la valeur de la directive. `Cache-Control: s-maxage` • Si `s-maxage` < TTL minimum, CloudFront met l'objet en cache pour la valeur du TTL CloudFront minimum. • Si `s-maxage` > TTL maximum, CloudFront met l'objet en cache pour la valeur du TTL CloudFront maximum. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache selon la valeur de la

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
		directive `Cache-Control: max-age`.

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
L'origine ajoute un en-tête **`Expires`**à l'objet	CloudFront mise en cache CloudFront met l'objet en cache jusqu'à la date indiquée dans l'`Expires`en-tête ou jusqu'à la valeur du TTL CloudFront maximum, selon la première éventualité. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache jusqu'à la date indiquée dans l'en-tête `Expires`.	CloudFront mise en cache CloudFront la mise en cache dépend des valeurs du TTL CloudFront minimum et du TTL maximum et de l'en-tête : `Expires` • Si TTL minimum < `Expires` < TTL maximum, l'objet est mis en CloudFront cache jusqu'à la date et à l'heure indiquées dans l'en-tête. `Expires` • Si `Expires` < TTL minimum, CloudFront met l'objet en cache pour la valeur du TTL CloudFront minimum. • Si `Expires` > TTL maximum, CloudFront met l'objet en cache pour la valeur du TTL CloudFront maximum. Conservation en cache par les navigateurs Les navigateurs mettent l'objet en cache jusqu'à la date et

En-têtes d'origine	Durée de vie minimale = 0	Durée de vie minimale > 0
		l'heure indiquées dans l'en-tête `Expires`.
Origin ajoute **`Cache-Control: no-cache no-store`** des and/or **`private`** directives à l'objet	CloudFront et les navigateurs respectent les en-têtes.	CloudFront mise en cache CloudFront met en cache l'objet pour la valeur du TTL CloudFront minimum. Voir l'avertissement en dessous de ce tableau. Conservation en cache par les navigateurs Les navigateurs respectent les en-têtes.

Warning

- Si votre TTL minimum est supérieur à 0, CloudFront utilise le TTL minimum de la politique de cache, même si les and/or `private` directives `Cache-Control: no-cacheno-store`, sont présentes dans les en-têtes d'origine.
  - Si l'origine est accessible, CloudFront récupère l'objet depuis l'origine et le renvoie au spectateur.
  - Si l'origine est inaccessible et que la valeur TTL minimale ou maximale est supérieure à 0, CloudFront servira l'objet qu'il a obtenu de l'origine précédemment.

  Pour éviter ce comportement, incluez la directive `Cache-Control: stale-if-error=0` avec l'objet renvoyé de l'origine. Cela CloudFront entraîne le renvoi d'une erreur en réponse aux demandes futures si l'origine est inaccessible, au lieu de renvoyer l'objet qu'il a obtenu de l'origine précédemment.
- CloudFront ne met pas en cache le code d'état HTTP 501 (non implémenté) provenant d'une origine S3 lorsque les en-têtes d'origine incluent les and/or `private`

directives`Cache-Control: no-cache,no-store,`. Il s'agit du comportement par défaut pour une origine S3, même si votre paramètre Durée de vie minimale est supérieur à 0.

Pour plus d'informations sur la façon de modifier les paramètres des distributions à l'aide de la CloudFront console, consultezMettre à jour une distribution. Pour plus d'informations sur la façon de modifier les paramètres des distributions à l'aide de l' CloudFront API, consultez UpdateDistribution.

Ajout d'en-têtes à vos objets à l'aide de la console Amazon S3

Vous pouvez ajouter le champ d'en-tête `Cache-Control` ou `Expires` à vos objets Amazon S3. Pour ce faire, vous devez modifier les champs de métadonnées de l'objet.

Pour ajouter un champ d'**`en-tête Cache-Control ou`** Expires aux objets Amazon S3

1. Suivez la procédure décrite dans la section Remplacement de métadonnées définies par le système de la rubrique Modification des métadonnées d'objet dans la console Amazon S3 du Guide de l'utilisateur Amazon S3.
2. Pour Key, choisissez le nom de l'en-tête que vous êtes en train d'ajouter (Cache-Controlou qui expire).
3. Dans Value (Valeur), entrez une valeur d'en-tête. Par exemple, pour une en-tête `Cache-Control`, vous pouvez entrer `max-age=86400`. Pour `Expires`, vous pouvez entrer une date et une heure d'expiration comme `Wed, 30 Jun 2021 09:28:00 GMT`.
4. Suivez le reste de la procédure pour enregistrer les modifications apportées aux métadonnées.

Mise en cache de contenu basée sur les paramètres de chaîne de requête

Certaines applications web utilisent des chaînes de requête pour envoyer des informations à l'origine. Une chaîne de requête est la partie d'une requête web qui s'affiche après un caractère ? ; la chaîne peut contenir un ou plusieurs paramètres séparés par des caractères &. Dans l'exemple suivant, la chaîne de requête inclut deux paramètres *`color=red`* et *`size=large`* :

`https://d111111abcdef8.cloudfront.net/images/image.jpg?`*`color=red&size=large`*

Pour les distributions, vous pouvez choisir si vous souhaitez transférer les chaînes de requête CloudFront vers votre origine et si vous souhaitez mettre en cache votre contenu en fonction de tous

les paramètres ou de paramètres sélectionnés. Pourquoi est-ce utile ? Prenez l'exemple de code suivant.

Supposons que votre site web soit disponible en cinq langues. La structure du répertoire et les noms de fichier des cinq versions du site web sont identiques. Lorsqu'un utilisateur consulte votre site Web, les demandes sont transmises pour CloudFront inclure un paramètre de chaîne de requête linguistique basé sur la langue choisie par l'utilisateur. Vous pouvez configurer CloudFront pour transmettre les chaînes de requête à l'origine et les mettre en cache en fonction du paramètre de langue. Si vous configurez votre serveur Web pour renvoyer la version d'une page donnée qui correspond à la langue sélectionnée, met en CloudFront cache chaque version linguistique séparément, en fonction de la valeur du paramètre de chaîne de requête linguistique.

Dans cet exemple, si la page principale de votre site Web est`main.html`, les cinq requêtes suivantes entraînent CloudFront la mise en cache `main.html` cinq fois, une fois pour chaque valeur du paramètre de chaîne de requête de langue :

- `https://d111111abcdef8.cloudfront.net/main.html?language=de`
- `https://d111111abcdef8.cloudfront.net/main.html?language=en`
- `https://d111111abcdef8.cloudfront.net/main.html?language=es`
- `https://d111111abcdef8.cloudfront.net/main.html?language=fr`
- `https://d111111abcdef8.cloudfront.net/main.html?language=jp`

Notez ce qui suit :

- Certains serveurs HTTP ne traitent pas les paramètres des chaînes de requête et ne renvoient donc pas de versions différentes d'un objet basé sur les valeurs des paramètres. Pour ces origines, si vous configurez pour CloudFront transmettre les paramètres de chaîne de requête à l'origine, la mise en cache se fait CloudFront toujours en fonction des valeurs des paramètres, même si l'origine renvoie des versions identiques de l'objet CloudFront pour chaque valeur de paramètre.
- Pour que les paramètres de chaîne de requête fonctionnent comme décrit dans l'exemple ci-dessus avec les langues, vous devez utiliser le caractère & comme délimiteur entre les paramètres de chaîne de requête. Si vous utilisez un délimiteur différent, vous risquez d'obtenir des résultats inattendus, en fonction des paramètres que vous spécifiez comme base pour la mise en cache et de l'ordre dans lequel les paramètres apparaissent dans la chaîne de requête. CloudFront

  Les exemples suivants montrent ce qui se passe si vous utilisez un délimiteur différent et que vous configurez CloudFront la mise en cache uniquement en fonction du `color` paramètre :

- Dans la requête suivante, met en CloudFront cache votre contenu en fonction de la valeur du `color` paramètre, mais CloudFront interprète cette valeur comme suit : *`red;size=large`*

  `https://d111111abcdef8.cloudfront.net/images/image.jpg?`*`color=red;size=large`*

- Dans la requête suivante, met en CloudFront cache votre contenu mais ne base pas la mise en cache sur les paramètres de la chaîne de requête. Cela est dû CloudFront au fait que vous avez configuré la mise en cache en fonction du `color` paramètre, mais que vous CloudFront interprétez la chaîne suivante comme contenant uniquement un `size` paramètre dont la *`large;color=red`* valeur est :

  `https://d111111abcdef8.cloudfront.net/images/image.jpg?`*`size=large;color=red`*

Vous pouvez configurer CloudFront pour effectuer l'une des opérations suivantes :

- Ne réachemine pas du tout les chaînes de requête vers l'origine. Si vous ne transférez pas les chaînes de requête, CloudFront ne met pas en cache en fonction des paramètres des chaînes de requête.
- Réachemine les chaînes de requête vers l'origine et mette en cache en fonction de tous les paramètres de la chaîne de requête.
- Réachemine les chaînes de requête vers l'origine et mette en cache en fonction des paramètres spécifiés de la chaîne de requête.

Pour plus d’informations, consultez the section called “Optimisation de la mise en cache”.

Rubriques

- Paramètres de console et d'API pour le réacheminement et la mise en cache des chaînes de requête
- Optimisation de la mise en cache
- Paramètres de chaîne de requête et journaux CloudFront standard (journaux d'accès)

Paramètres de console et d'API pour le réacheminement et la mise en cache des chaînes de requête

Lorsque vous créez une distribution dans la CloudFront console, CloudFront configure le transfert et la mise en cache des chaînes de requête pour vous en fonction de votre type d'origine. Vous pouvez, si vous le souhaitez, modifier manuellement ces paramètres. Pour plus d'informations, consultez les paramètres suivantes dans le the section called "Tous les paramètres de distribution" :

- the section called "Réacheminement et mise en cache des chaînes de requête"
- the section called "Liste d'autorisation des chaînes de requête"

Pour configurer le transfert et la mise en cache des chaînes de requête avec l' CloudFront API, consultez CachePolicy et OriginRequestPolicy dans le Amazon CloudFront API Reference.

Optimisation de la mise en cache

Lorsque vous configurez CloudFront la mise en cache en fonction des paramètres de chaîne de requête, vous pouvez prendre les mesures suivantes pour réduire le nombre de demandes qui CloudFront sont transmises à votre origine. Lorsque les emplacements CloudFront périphériques desservent des objets, vous réduisez la charge sur votre serveur d'origine et vous réduisez la latence, car les objets sont servis depuis des emplacements plus proches de vos utilisateurs.

Mettre en cache uniquement sur des paramètres pour lesquels votre origine renvoie des versions différentes d'un objet

Pour chaque paramètre de chaîne de requête vers lequel votre application Web transmet CloudFront les CloudFront demandes à votre origine pour chaque valeur de paramètre et met en cache une version distincte de l'objet pour chaque valeur de paramètre. Ceci est le cas même si votre origine renvoie toujours le même objet quelle que soit la valeur du paramètre. Dans le cas de plusieurs paramètres, le nombre de requêtes et le nombre d'objets sont multipliés.

Nous vous recommandons de CloudFront configurer la mise en cache uniquement en fonction des paramètres de chaîne de requête pour lesquels votre origine renvoie différentes versions, et d'examiner attentivement les avantages de la mise en cache en fonction de chaque paramètre. Par exemple, supposons que vous ayez un site web de vente au détail. Vous présentez les photos d'une veste dans six couleurs différentes et cette veste est disponible dans 10 tailles. Les photos que vous affichez pour la veste montrent les différentes couleurs proposées, mais pas les différentes tailles. Pour optimiser la mise en cache, vous CloudFront devez configurer la mise

en cache en fonction uniquement du paramètre de couleur, et non du paramètre de taille. Cela augmente la probabilité qu'une demande CloudFront puisse être traitée depuis le cache, ce qui améliore les performances et réduit la charge sur votre origine.

Toujours répertorier les paramètres dans le même ordre

L'ordre des paramètres a de l'importance dans les chaînes de requête. Dans l'exemple suivant, les chaînes de requête sont identiques, mais les paramètres sont dans un ordre différent. Cela CloudFront entraîne le transfert de deux requêtes distinctes pour image.jpg à votre origine et la mise en cache de deux versions distinctes de l'objet :

- `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=red&size=large`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large&color=red`

Nous vous recommandons de toujours utiliser le même ordre pour la liste des noms de paramètres, par exemple l'ordre alphabétique.

Toujours utiliser la même casse pour les noms et les valeurs des paramètres

CloudFront considère le cas des noms et des valeurs des paramètres lors de la mise en cache en fonction des paramètres de chaîne de requête. Dans l'exemple suivant, les chaînes de requête sont identiques sauf dans le cas des noms et des valeurs des paramètres. Cela CloudFront entraîne le transfert de quatre requêtes distinctes pour image.jpg à votre origine et la mise en cache de quatre versions distinctes de l'objet :

- `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=red`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?color=Red`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?Color=red`
- `https://d111111abcdef8.cloudfront.net/images/image.jpg?Color=Red`

Nous vous recommandons d'utiliser systématiquement la même casse pour les noms et valeurs des paramètres, par exemple des minuscules.

N'utilisez pas de noms de paramètres qui soient en conflit avec les URL signées

Si vous utilisez des URL signées pour restreindre l'accès à votre contenu (si vous avez ajouté des signataires de confiance à votre distribution), CloudFront supprimez les paramètres de chaîne de requête suivants avant de transférer le reste de l'URL vers votre origine :

- `Expires`

- `Key-Pair-Id`
- `Policy`
- `Signature`

Si vous utilisez des URL signées et que vous souhaitez les configurer CloudFront pour transférer les chaînes de requête vers votre origine, les paramètres de vos propres chaînes de requête ne peuvent pas être nommés `Expires` `Key-Pair-Id``Policy`,, ou`Signature`.

Paramètres de chaîne de requête et journaux CloudFront standard (journaux d'accès)

Si vous activez la journalisation, CloudFront enregistre l'URL complète, y compris les paramètres de chaîne de requête. Cela est vrai, que vous ayez configuré pour transmettre CloudFront les chaînes de requête à l'origine ou non. Pour plus d'informations sur la CloudFront journalisation, consultezthe section called “Journaux d'accès (journaux standard)”.

Mise en cache de contenu basée sur des cookies

Par défaut, CloudFront ne prend pas en compte les cookies lors du traitement des demandes et des réponses, ou lors de la mise en cache de vos objets dans des emplacements périphériques. Si CloudFront reçoit deux demandes identiques à l'exception du contenu de l'`Cookie`en-tête, alors, par défaut, les demandes CloudFront sont traitées comme identiques et renvoie le même objet pour les deux demandes.

Vous pouvez configurer CloudFront pour transmettre à votre origine une partie ou la totalité des cookies dans les requêtes des utilisateurs, et pour mettre en cache des versions distinctes de vos objets en fonction des valeurs des cookies qu'ils transmettent. Dans ce cas, CloudFront utilise une partie ou la totalité des cookies contenus dans les demandes des utilisateurs, quels que soient ceux qu'il est configuré pour transférer, afin d'identifier de manière unique un objet dans le cache.

Par exemple, supposons que des demandes pour `locations.html` contiennent un cookie `country` ayant la valeur uk ou `fr`. Lorsque vous configurez CloudFront la mise en cache de vos objets en fonction de la valeur du `country` cookie CloudFront , transmettez les demandes `locations.html` à l'origine et incluez le `country` cookie et sa valeur. Votre origine renvoie `locations.html` l'objet et le CloudFront met en cache une fois pour les requêtes contenant la valeur du `country` cookie uk et une fois pour les requêtes contenant cette valeur. `fr`

> **Important**
>
> Amazon S3 et certains serveurs HTTP ne gèrent pas les cookies. Ne configurez pas CloudFront pour transférer les cookies vers une origine qui ne traite pas les cookies ou qui ne modifie pas sa réponse en fonction des cookies. Cela peut CloudFront entraîner le transfert d'un plus grand nombre de demandes vers l'origine pour le même objet, ce qui ralentit les performances et augmente la charge sur l'origine. Si, compte tenu de l'exemple précédent, votre site d'origine ne traite pas le `country` cookie ou renvoie toujours la même version de `locations.html` to, CloudFront quelle que soit la valeur du `country` cookie, ne configurez pas CloudFront pour transférer ce cookie.
>
> À l'inverse, si votre origine personnalisée dépend d'un cookie en particulier ou envoie des réponses différentes en fonction d'un cookie, assurez-vous de le configurer CloudFront pour transférer ce cookie vers l'origine. Dans le cas contraire, CloudFront supprimez le cookie avant de transmettre la demande à votre adresse d'origine.

Pour configurer la transmission des cookies, vous mettez à jour le comportement du cache de votre distribution. Pour de plus amples informations sur les comportements de cache, consultez Paramètres de comportement du cache, en particulier les sections Réacheminer les cookies et Cookies de la liste d'autorisation.

Vous pouvez configurer chaque comportement de cache pour effectuer l'une des opérations suivantes :

- Transférer tous les cookies vers votre origine : CloudFront inclut tous les cookies envoyés par l'utilisateur lorsqu'il transmet des demandes à l'origine. Lorsque votre origine renvoie une réponse, met la réponse en CloudFront cache à l'aide des noms et des valeurs des cookies contenus dans la demande de l'utilisateur. Si la réponse d'origine inclut `Set-Cookie` des en-têtes, les CloudFront renvoie au visualiseur avec l'objet demandé. CloudFront met également en cache `Set-Cookie` les en-têtes contenant l'objet renvoyé par l'origine et envoie ces `Set-Cookie` en-têtes aux spectateurs à chaque accès au cache.
- Transférer un ensemble de cookies que vous spécifiez : CloudFront supprime tous les cookies envoyés par l'utilisateur qui ne figurent pas sur la liste autorisée avant de transmettre une demande à l'origine. CloudFront met en cache la réponse en utilisant les noms et valeurs des cookies répertoriés dans la demande de l'utilisateur. Si la réponse d'origine inclut `Set-Cookie` des en-têtes, les CloudFront renvoie au visualiseur avec l'objet demandé. CloudFront met également en

cache `Set-Cookie` les en-têtes contenant l'objet renvoyé par l'origine et envoie ces `Set-Cookie` en-têtes aux spectateurs à chaque accès au cache.

Pour plus d'informations sur la spécification de caractères génériques dans des noms des cookies, consultez Cookies de la liste d’autorisation.

Pour déterminer le quota actuel concernant le nombre de noms de cookies que vous pouvez transférer pour chaque comportement de cache ou pour demander un quota supérieur, consultez la section Quotas sur les chaînes de requêtes (paramètres de cache hérités).

- Ne transférez pas les cookies vers votre site d'origine : vos objets CloudFront ne sont pas mis en cache en fonction des cookies envoyés par le visiteur. En outre, CloudFront supprime les cookies avant de transmettre les demandes à votre source et supprime les `Set-Cookie` en-têtes des réponses avant de renvoyer les réponses à vos spectateurs. Étant donné qu’il ne s’agit pas d’un mode d’utilisation optimal des ressources de l’origine, lorsque vous choisissez ce comportement de cache, veillez à ce que votre origine n’ajoute pas de cookies par défaut dans ses réponses.

Remarque à propos de la spécification des cookies que vous ne souhaitez pas transmettre :

Journaux d'accès

Si vous configurez CloudFront pour enregistrer les demandes et pour enregistrer les cookies, CloudFront enregistre tous les cookies et tous les attributs des cookies, même si vous configurez pour CloudFront ne pas transférer les cookies vers votre origine ou si vous configurez CloudFront pour ne transférer que des cookies spécifiques. Pour plus d'informations sur la CloudFront journalisation, consultezJournaux d'accès (journaux standard).

Sensibilité à la casse

Les noms et valeurs de cookie sont sensibles à la casse. Par exemple, s'il CloudFront est configuré pour transférer tous les cookies et que deux requêtes de l'utilisateur pour le même objet contiennent des cookies identiques à l'exception des majuscules, l'objet est mis en CloudFront cache deux fois.

CloudFront trie les cookies

CloudFront Il est configuré pour transférer les cookies (tous ou un sous-ensemble), CloudFront trie les cookies dans l'ordre naturel par nom de cookie avant de transmettre la demande à votre source.

> **Note**
>
> Les noms de cookies commençant par un $ caractère ne sont pas pris en charge. CloudFront supprimera le cookie avant de transmettre la demande à l'origine. Vous pouvez supprimer le caractère $ ou en spécifier un autre au début du nom du cookie.

`If-Modified-Since` et `If-None-Match`

`If-Modified-Since`et les requêtes `If-None-Match` conditionnelles ne sont pas prises en charge lorsqu'il CloudFront est configuré pour transférer les cookies (tous ou un sous-ensemble).

Un format standard de paire nom-valeur est requis

CloudFront transmet un en-tête de cookie uniquement si la valeur est conforme au format standard de paire nom-valeur, par exemple : `"Cookie: cookie1=value1; cookie2=value2"`

Désactiver la mise en cache des en-têtes **`Set-Cookie`**

S'il CloudFront est configuré pour transférer les cookies vers l'origine (qu'il s'agisse de cookies complets ou spécifiques), il met également en cache les `Set-Cookie` en-têtes reçus dans la réponse d'origine. CloudFront inclut ces `Set-Cookie` en-têtes dans sa réponse au visualiseur d'origine et les inclut également dans les réponses suivantes qui sont diffusées depuis le CloudFront cache.

Si vous souhaitez recevoir des cookies à votre origine mais que vous ne souhaitez pas CloudFront mettre en cache `Set-Cookie` les en-têtes des réponses de votre origine, configurez votre origine pour ajouter un `Cache-Control` en-tête avec une `no-cache` directive qui le spécifie `Set-Cookie` comme nom de champ. Par exemple : `Cache-Control: no-cache="Set-Cookie"`. Pour plus d'informations, consultez la section Cache-Control Directives de réponse dans le protocole de transfert hypertexte (HTTP/1.1) : norme de mise en cache.

Longueur maximum des noms de cookie

Si vous configurez CloudFront pour transférer des cookies spécifiques vers votre origine, le nombre total d'octets dans tous les noms de cookies que vous configurez CloudFront pour transférer ne peut pas dépasser 512 moins le nombre de cookies que vous transférez. Par exemple, si vous configurez CloudFront pour transférer 10 cookies vers votre site d'origine, la longueur combinée des noms des 10 cookies ne peut pas dépasser 502 octets (512 à 10).

Si vous configurez CloudFront pour transférer tous les cookies vers votre origine, la longueur des noms des cookies n'a pas d'importance.

Pour plus d'informations sur l'utilisation de la CloudFront console pour mettre à jour une distribution CloudFront afin de transmettre les cookies à l'origine, consultezMettre à jour une distribution. Pour plus d'informations sur l'utilisation de l' CloudFront API pour mettre à jour une distribution, consultez UpdateDistribution le manuel Amazon CloudFront API Reference.

Mise en cache de contenu basée sur des en-têtes de demandes

Avec CloudFront, vous pouvez choisir de transférer les en-têtes CloudFront vers votre origine et de mettre en cache des versions distinctes d'un objet spécifié en fonction des valeurs d'en-tête des requêtes des spectateurs. Vous pouvez ainsi diffuser différentes versions de votre contenu en fonction de l'appareil utilisé par l'utilisateur, de l'emplacement du spectateur, de la langue utilisée par le spectateur et de divers autres critères.

Rubriques

- En-têtes et distributions web : présentation
- Sélection des en-têtes sur lesquels baser la mise en cache
- Configurer CloudFront pour respecter les paramètres CORS
- Configuration de la mise en cache en fonction du type d’appareil
- Configuration de la mise en cache en fonction de la langue de l’utilisateur
- Configuration de la mise en cache en fonction de l’emplacement de l’utilisateur
- Configuration de la mise en cache en fonction du protocole de la demande
- Configuration de mise en cache pour les fichiers compressés
- Incidence de la mise en cache basée sur les en-têtes sur les performances
- Impact de la casse des en-têtes et des valeurs d'en-tête sur la mise en cache
- En-têtes qui CloudFront renvoient au visualiseur

En-têtes et distributions web : présentation

Par défaut, les en-têtes CloudFront ne sont pas pris en compte lors de la mise en cache de vos objets dans des emplacements périphériques. Si votre origine renvoie deux objets et que ceux-ci

ne diffèrent que par les valeurs des en-têtes de demande, une seule version de l'objet est mise en CloudFront cache.

Vous pouvez configurer CloudFront pour transférer les en-têtes vers l'origine, ce qui entraîne la mise CloudFront en cache de plusieurs versions d'un objet en fonction des valeurs d'un ou de plusieurs en-têtes de demande. CloudFront Pour configurer la mise en cache des objets en fonction des valeurs d'en-têtes spécifiques, vous devez spécifier les paramètres de comportement du cache pour votre distribution. Pour plus d'informations, consultez Mise en cache basée sur des en-têtes de requête sélectionnés.

Par exemple, supposons que des demandes d'utilisateur pour `logo.jpg` contiennent un en-tête `Product` personnalisé ayant la valeur `Acme` ou `Apex`. Lorsque vous configurez CloudFront la mise en cache de vos objets en fonction de la valeur de l'`Producten`-tête, CloudFront transférez les demandes `logo.jpg` à l'origine et incluez l'`Producten`-tête et les valeurs d'en-tête. CloudFront met en cache `logo.jpg` une fois pour les requêtes contenant la valeur de l'`Producten`-tête `Acme` et une fois pour les requêtes contenant cette valeur. `Apex`

Vous pouvez configurer chaque comportement de cache d'une distribution pour exécuter l'une des opérations suivantes :

- Transmettre tous les en-têtes à votre origine

  > **Note**
  >
  > Pour les anciens paramètres de cache : si vous configurez CloudFront pour transférer tous les en-têtes vers votre origine, les objets associés à ce comportement de cache CloudFront ne sont pas mis en cache. Par contre, il envoie chaque demande à l'origine.

- Transférez la liste des en-têtes que vous spécifiez. CloudFront met en cache vos objets en fonction des valeurs de tous les en-têtes spécifiés. CloudFront transmet également les en-têtes qu'il transmet par défaut, mais il met en cache vos objets uniquement en fonction des en-têtes que vous spécifiez.
- Transmettre uniquement les en-têtes par défaut. Dans cette configuration, vos objets CloudFront ne sont pas mis en cache en fonction des valeurs des en-têtes de demande.

Pour obtenir le quota actuel relatif au nombre d'en-têtes que vous pouvez transférer pour chaque comportement de cache ou pour demander un quota supérieur, consultez la section Quotas sur les en-têtes.

Pour plus d'informations sur l'utilisation de la CloudFront console pour mettre à jour une distribution afin CloudFront de transmettre les en-têtes à l'origine, consultezMettre à jour une distribution. Pour plus d'informations sur l'utilisation de l' CloudFrontAPI pour mettre à jour une distribution existante, consultez la section Mettre à jour la distribution dans le Amazon CloudFront API Reference.

Sélection des en-têtes sur lesquels baser la mise en cache

Les en-têtes que vous pouvez transmettre à l'origine et sur lesquels repose CloudFront la mise en cache varient selon que votre origine est un compartiment Amazon S3 ou une origine personnalisée.

- Amazon S3 — Vous pouvez configurer CloudFront pour transférer et mettre en cache vos objets en fonction d'un certain nombre d'en-têtes spécifiques (voir la liste d'exceptions suivante). Toutefois, nous vous recommandons d'éviter de transférer des en-têtes avec une origine Amazon S3, sauf si vous devez implémenter le partage des ressources cross-origin (CORS) ou que vous souhaitez personnaliser du contenu en utilisant Lambda@Edge dans les événements axés sur l'origine.
  - Pour configurer CORS, vous devez transférer des en-têtes qui permettent CloudFront de distribuer du contenu pour les sites Web qui sont activés pour le partage de ressources entre origines (CORS). Pour plus d'informations, consultez Configurer CloudFront pour respecter les paramètres CORS.
  - Pour personnaliser le contenu à l'aide d'en-têtes que vous transférez vers votre origine Amazon S3, vous écrivez et ajoutez des fonctions Lambda @Edge et vous les associez à votre CloudFront distribution qui sera déclenchée par un événement lié à l'origine. Pour plus d'informations sur l'utilisation des en-têtes afin de personnaliser du contenu, consultez Personnalisation de contenu à l'aide des en-têtes Pays ou Type d'appareil – exemples.

    Nous vous recommandons d'éviter de transférer des en-têtes que vous n'utilisez pas pour personnaliser du contenu, car le transfert d'en-têtes supplémentaires peut réduire votre taux d'accès au cache. En d'autres termes, il ne CloudFront peut pas traiter autant de demandes provenant de caches périphériques que par rapport à l'ensemble des demandes.
- Origine personnalisée : vous pouvez configurer la mise CloudFront en cache en fonction de la valeur de n'importe quel en-tête de demande, à l'exception des suivants :
  - `Connection`
  - `Cookie` – Si vous souhaitez effectuer la transmission et la mise en cache en fonction de cookies, vous utilisez un paramètre distinct dans votre distribution. Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.
  - `Host (for Amazon S3 origins)`

- `Proxy-Authorization`
- `TE`
- `Upgrade`

Vous pouvez CloudFront configurer la mise en cache des objets en fonction des valeurs `User-Agent` des en-têtes `Date` et, mais nous ne le recommandons pas. Ces en-têtes ont de nombreuses valeurs possibles, et la mise en cache basée sur leurs valeurs peut entraîner le transfert d'un plus grand nombre de demandes CloudFront vers votre origine.

Pour obtenir la liste complète des en-têtes de requêtes HTTP et la manière dont ils CloudFront sont traités, consultezEn-têtes et CloudFront comportement des requêtes HTTP (origines personnalisées et Amazon S3).

Configurer CloudFront pour respecter les paramètres CORS

Si vous avez activé le partage des ressources cross-origin (CORS) dans un compartiment Amazon S3 ou une origine personnalisée, vous devez choisir des en-têtes spécifiques à transmettre pour respecter les paramètres CORS. Les en-têtes que vous devez transférer diffèrent en fonction de l'origine (Amazon S3 ou origine personnalisée) et selon que vous souhaitez ou non mettre en cache les réponses `OPTIONS`.

Amazon S3

- Si vous souhaitez que les réponses `OPTIONS` soient mises en cache, procédez comme suit :
  - Choisissez les options pour les paramètres de comportement de cache par défaut qui permettent la mise en cache pour les réponses `OPTIONS`.
  - Configurez CloudFront pour transférer les en-têtes suivants : `Origin`Access-Control-Request-Headers, et`Access-Control-Request-Method`.
- Si vous ne voulez pas que les réponses `OPTIONS` soient mises en cache, configurez CloudFront de sorte à réacheminer l'en-tête `Origin`, ainsi que tous les autres en-têtes requis par votre origine (`Access-Control-Request-Headers` ou `Access-Control-Request-Method` par exemple).

Origines personnalisées – Transmettez l'en-tête `Origin` en même temps que tous les autres en-têtes requis par votre origine.

CloudFront Pour configurer la mise en cache des réponses basées sur CORS, vous devez configurer CloudFront pour transférer les en-têtes à l'aide d'une politique de cache. Pour plus d'informations, consultez Contrôle de la clé de cache à l'aide d'une politique.

Pour plus d'informations sur CORS et Amazon S3, consultez la section Utilisation du partage des ressources cross-origin (CORS) du Guide de l'utilisateur Amazon Simple Storage Service.

Configuration de la mise en cache en fonction du type d'appareil

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction de l'appareil qu'un utilisateur utilise pour afficher votre contenu, configurez CloudFront pour transférer les en-têtes applicables vers votre origine personnalisée :

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

En fonction de la valeur de l'`User-Agent`en-tête, CloudFront définit la valeur de ces en-têtes à `true` ou `false` avant de transmettre la demande à votre origine. Si un appareil entre dans plusieurs catégories, plusieurs valeurs peuvent être `true`. Par exemple, pour certaines tablettes, CloudFront vous pouvez définir `CloudFront-Is-Tablet-Viewer` à la fois `CloudFront-Is-Mobile-Viewer` et sur`true`.

Configuration de la mise en cache en fonction de la langue de l'utilisateur

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction de la langue spécifiée dans la demande, configurez CloudFront pour transmettre l'`Accept-Language`en-tête à votre origine.

Configuration de la mise en cache en fonction de l'emplacement de l'utilisateur

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction du pays d'origine de la demande, configurez CloudFront pour transférer l'`CloudFront-Viewer-Country`en-tête vers votre origine. CloudFront convertit automatiquement l'adresse IP d'origine de la demande en un code de pays à deux lettres. Pour accéder à une liste de codes pays facile à utiliser et pouvant être triée par code et nom de pays, consultez l'entrée Wikipedia ISO 3166-1 alpha-2.

Configuration de la mise en cache en fonction du protocole de la demande

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction du protocole de la requête, HTTP ou HTTPS, configurez CloudFront pour transmettre l'`CloudFront-Forwarded-Proto`en-tête à votre origine.

Configuration de mise en cache pour les fichiers compressés

Si votre origine prend en charge la compression Brotli, vous pouvez effectuer une mise en cache en fonction de l'en-tête `Accept-Encoding`. Configurez la mise en cache en fonction de `Accept-Encoding` uniquement si votre origine traite différents contenus selon l'en-tête.

Incidence de la mise en cache basée sur les en-têtes sur les performances

Lorsque vous configurez CloudFront la mise en cache en fonction d'un ou de plusieurs en-têtes et que les en-têtes ont plusieurs valeurs possibles, CloudFront vous transférez d'autres demandes à votre serveur d'origine pour le même objet. Ceci ralentit les performances et augmente la charge sur votre serveur d'origine. Si votre serveur d'origine renvoie le même objet quelle que soit la valeur d'un en-tête donné, nous vous recommandons de ne pas configurer la mise CloudFront en cache en fonction de cet en-tête.

Si vous configurez CloudFront pour transférer plusieurs en-têtes, l'ordre des en-têtes dans les requêtes des spectateurs n'affecte pas la mise en cache tant que les valeurs sont les mêmes. Par exemple, si une demande contient les en-têtes A:1 B:2 et qu'une autre en contientB:2,A:1, met en CloudFront cache une seule copie de l'objet.

Impact de la casse des en-têtes et des valeurs d'en-tête sur la mise en cache

Lorsque CloudFront les caches sont basés sur des valeurs d'en-tête, il ne prend pas en compte le cas du nom de l'en-tête, mais le cas de la valeur de l'en-tête :

- Si les demandes de l'utilisateur incluent à la fois `Product:Acme` et`product:Acme`, ne met en CloudFront cache un objet qu'une seule fois. La seule différence entre les deux est la casse du nom de l'en-tête qui n'a pas d'incidence sur la mise en cache.
- Si les demandes de l'utilisateur incluent à la fois `Product:Acme` et`Product:acme`, un objet est mis en CloudFront cache deux fois, car la valeur se trouve `Acme` dans certaines requêtes et `acme` dans d'autres.

En-têtes qui CloudFront renvoient au visualiseur

La configuration CloudFront pour transférer et mettre en cache les en-têtes n'a aucune incidence sur les en-têtes CloudFront renvoyés au visualiseur. CloudFront renvoie tous les en-têtes qu'il obtient de l'origine à quelques exceptions près. Pour plus d'informations, consultez la rubrique applicable :

- Origines Amazon S3 — Voir en-têtes de réponse HTTP qui CloudFront suppriment ou mettent à jour.
- Origines personnalisées – Voir en-têtes de réponse HTTP qui CloudFront suppriment ou remplacent.

Contrôle de la clé de cache à l'aide d'une politique

Avec une politique de CloudFront cache, vous pouvez spécifier les en-têtes HTTP, les cookies et les chaînes de requête CloudFront inclus dans la clé de cache pour les objets mis en cache à des emplacements CloudFront périphériques. La clé de cache est l'identifiant unique de chaque objet du cache, et elle détermine si la demande HTTP d'un utilisateur entraîne un accès au cache.

Un accès au cache se produit lorsqu'une demande d'utilisateur génère la même clé de cache qu'une requête précédente et que l'objet de cette clé de cache est dans le cache de l'emplacement périphérique et valide. En cas d'accès au cache, l'objet est diffusé au spectateur depuis un emplacement CloudFront périphérique, ce qui présente les avantages suivants :

- Réduction de la charge sur votre serveur d'origine
- Latence réduite pour l'utilisateur

L'inclusion de moins de valeurs dans la clé de cache augmente la probabilité d'un accès au cache. Vous obtenez ainsi de meilleures performances à partir de votre site web ou de votre application, car le taux d'accès au cache augmente (une proportion plus élevée de demandes de l'utilisateur entraîne un accès au cache). Pour de plus amples informations, veuillez consulter Comprendre la clé de cache.

Pour contrôler la clé de cache, vous devez utiliser une politique de CloudFront cache. Vous associez une politique de cache à un ou plusieurs comportements de cache dans une CloudFront distribution.

Vous pouvez également utiliser la politique de cache pour spécifier les paramètres de durée de vie (TTL) des objets du CloudFront cache et permettre de demander et de CloudFront mettre en cache des objets compressés.

> **Note**
>
> Les paramètres du cache n'ont aucun effet sur les demandes gRPC, car le trafic gRPC ne peut pas être mis en cache. Pour de plus amples informations, veuillez consulter Utilisation de gRPC avec des distributions CloudFront.

Rubriques

- Compréhension des politiques de cache

- Création de politiques de cache
- Utilisation des politiques de cache gérées
- Comprendre la clé de cache

Compréhension des politiques de cache

Vous pouvez utiliser une stratégie de cache pour améliorer votre taux d'accès du cache en contrôlant les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) incluses dans la clé de cache. CloudFront fournit des stratégies de cache prédéfinies, nommées stratégies gérées, pour les cas d'utilisation courants. Vous pouvez utiliser ces politiques gérées ou créer votre propre politique de cache adaptée à vos besoins. Pour plus d'informations sur les stratégies gérées, consultez Utilisation des politiques de cache gérées.

Une politique de cache contient les paramètres suivants, qui sont classés en informations de politique, paramètres time-to-live (TTL) et paramètres de clé de cache.

Informations sur les politiques

Nom

Nom permettant d'identifier la politique de cache. Dans la console, vous utilisez le nom pour attacher la politique de cache à un comportement de cache.

Description

Commentaire décrivant la politique de cache. Cette option est facultative, mais elle peut vous aider à identifier l'objectif de la politique de cache.

Paramètres time-to-live (TTL)

Les paramètres de durée de vie (TTL) fonctionnent conjointement avec les en-têtes `Cache-Control` et `Expires` HTTP (s'ils figurent dans la réponse d'origine) pour déterminer la durée de validité des objets du CloudFront cache.

Durée de vie minimale

Durée minimale, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de CloudFront vérifier auprès de l'origine si l'objet a été mis à jour. Pour

de plus amples informations, veuillez consulter Gestion de la durée de conservation de contenu dans le cache (expiration).

> **Warning**
>
> Si votre TTL minimum est supérieur à 0, le contenu CloudFront sera mis en cache pendant au moins la durée spécifiée dans le TTL minimum de la politique de cache, même si les `private` directives `Cache-Control: no-cacheno-store`, ou sont présentes dans les en-têtes d'origine.

Durée de vie (TTL) maximale

Durée maximale, en secondes, pendant laquelle les objets restent dans le CloudFront cache avant de CloudFront vérifier auprès de l'origine si l'objet a été mis à jour. CloudFront utilise ce paramètre uniquement lorsque l'origine envoie `Cache-Control` ou contient `Expires` des en-têtes avec l'objet. Pour de plus amples informations, veuillez consulter Gestion de la durée de conservation de contenu dans le cache (expiration).

TTL par défaut

Durée par défaut, en secondes, pendant laquelle vous souhaitez que les objets restent dans le CloudFront cache avant de CloudFront vérifier auprès de l'origine si l'objet a été mis à jour. CloudFront utilise la valeur de ce paramètre comme TTL de l'objet uniquement lorsque l'origine n'envoie pas *`Cache-Control`* ou ne contient pas d'`Expires`en-têtes avec l'objet. Pour de plus amples informations, veuillez consulter Gestion de la durée de conservation de contenu dans le cache (expiration).

> **Note**
>
> Si les paramètres TTL minimum, TTL maximum et TTL par défaut sont tous définis sur 0, la mise en cache est désactivée. CloudFront

Paramètres de la clé de cache

Les paramètres de la clé de cache spécifient les valeurs figurant dans les demandes du lecteur CloudFront incluses dans la clé de cache. Les valeurs peuvent inclure des chaînes de requête

URL, des en-têtes HTTP et des cookies. Les valeurs que vous incluez dans la clé de cache sont automatiquement incluses dans les demandes CloudFront envoyées à l'origine, nommées demandes d'origine. Pour plus d'informations sur le contrôle des demandes d'origine sans affecter la clé de cache, consultez Contrôle des demandes d'origine à l'aide d'une stratégie.

Les paramètres de clé de cache incluent :

- En-têtes
- Cookies
- Chaînes de requête
- Prise en charge de la compression

En-têtes

Les en-têtes HTTP dans les demandes du lecteur, CloudFront y compris dans la clé de cache et dans les demandes d'origine. Pour les en-têtes, vous pouvez choisir l'un des paramètres suivants :

- Aucun – Les en-têtes HTTP dans les demandes de l'utilisateur ne sont pas inclus dans la clé de cache et ne sont pas automatiquement inclus dans les demandes d'origine.
- Include the following headers (Inclure les en-têtes suivants) – Vous spécifiez quels en-têtes HTTP des demandes de l'utilisateur sont inclus dans la clé de cache et automatiquement inclus dans les demandes d'origine.

Lorsque vous utilisez le paramètre Include the following headers (Inclure les en-têtes suivants), vous spécifiez les en-têtes HTTP par leur nom, et non par leur valeur. Par exemple, considérez l'en-tête HTTP suivant :

```
Accept-Language: en-US,en;q=0.5
```

Dans ce cas, vous spécifiez l'en-tête comme `Accept-Language`, pas comme `Accept-Language: en-US,en;q=0.5`. Toutefois, CloudFront inclut l'en-tête complet, y compris sa valeur, dans la clé de cache et dans les demandes d'origine.

Vous pouvez également inclure certains en-têtes générés par CloudFront dans la clé de cache. Pour de plus amples informations, veuillez consulter the section called “Ajouter des en-têtes de CloudFront demande”.

Cookies

Les cookies contenus dans les demandes du lecteur, CloudFront y compris dans la clé de cache, et dans les demandes d'origine. Pour les cookies, vous pouvez choisir l'un des paramètres suivants :

- Aucun – Les cookies dans les demandes de l'utilisateur ne sont pas inclus dans la clé de cache et ne sont pas automatiquement inclus dans les demandes d'origine.
- Tous – Tous les cookies dans les demandes de l'utilisateur sont inclus dans la clé de cache et sont automatiquement inclus dans les demandes d'origine.
- Include specified cookies (Inclure les cookies spécifiés) – Vous spécifiez quels cookies dans les demandes de l'utilisateur sont inclus dans la clé de cache et automatiquement inclus dans les demandes d'origine.
- Include all cookies except (Inclure tous les cookies sauf) – Vous spécifiez quels cookies dans les demandes de l'utilisateur ne sont pas inclus dans la clé de cache et ne sont pas automatiquement inclus dans les demandes d'origine. Tous les autres cookies, à l'exception de ceux que vous spécifiez, sont inclus dans la clé de cache et automatiquement inclus dans les demandes d'origine.

Lorsque vous utilisez le paramètre Include specified cookies (Inclure les cookies spécifiés) ou Include all cookies except (Inclure tous les cookies sauf), vous spécifiez les cookies par leur nom, et non par leur valeur. Prenons l'exemple de l'en-tête `Cookie` suivant :

```
Cookie: session_ID=abcd1234
```

Dans ce cas, vous spécifiez le cookie comme `session_ID`, pas comme `session_ID=abcd1234`. Cependant, CloudFront inclut le cookie complet, y compris sa valeur, dans la clé de cache et dans les requêtes d'origine.

Chaînes de requête

Les chaînes de requête d'URL contenues dans les demandes du lecteur CloudFront incluses dans la clé de cache et dans les demandes d'origine. Pour les chaînes de requête, vous pouvez choisir l'un des paramètres suivants :

- Aucun – Les chaînes de requête dans les demandes utilisateur ne sont pas incluses dans la clé de cache et ne sont pas automatiquement incluses dans les demandes d'origine.
- Toutes – Toutes les chaînes de requête dans les demandes de l'utilisateur sont incluses dans la clé de cache et sont également automatiquement incluses dans les demandes d'origine.

- Include specified query strings (Inclure les chaînes de requête spécifiées) – Vous spécifiez quelles chaînes de requête dans les demandes de l'utilisateur sont incluses dans la clé de cache et automatiquement incluses dans les demandes d'origine.
- Include all query strings except (Inclure toutes les chaînes de requête sauf) – Vous spécifiez quelles chaînes de requête dans les demandes de l'utilisateur ne sont pas incluses dans la clé de cache et ne sont pas automatiquement incluses dans les demandes d'origine. Toutes les autres chaînes de requête, à l'exception de celles que vous spécifiez, sont incluses dans la clé de cache et automatiquement incluses dans les demandes d'origine.

Lorsque vous utilisez le paramètres Include specified query strings (Inclure les chaînes de requête spécifiées) Include all query strings except (Inclure toutes les chaînes de requête sauf), vous spécifiez les chaînes de requête par leur nom, et non par leur valeur. Prenons l'exemple du chemin d'URL suivant :

```
/content/stories/example-story.html?split-pages=false
```

Dans ce cas, vous spécifiez la chaîne de requête comme `split-pages`, pas comme `split-pages=false`. Cependant, CloudFront inclut la chaîne de requête complète, y compris sa valeur, dans la clé de cache et dans les demandes d'origine.

> **Note**
>
> Pour les paramètres des clés de cache, CloudFront traitez l'astérisque (*) pour les en-têtes, les chaînes de requête et les cookies comme une chaîne littérale et non comme un caractère générique.

Prise en charge de la compression

Ces paramètres permettent CloudFront de demander et de mettre en cache des objets compressés aux formats de compression Gzip ou Brotli, lorsque le visualiseur les prend en charge. Ces paramètres permettent également à la compression CloudFront de fonctionner. Les utilisateurs indiquent leur prise en charge de ces formats de compression avec l'en-tête `Accept-Encoding` HTTP.

> **Note**
>
> Les navigateurs web Chrome et Firefox prennent en charge la compression Brotli uniquement lorsque la demande est envoyée en HTTPS. Ces navigateurs ne prennent pas en charge Brotli avec les demandes HTTP.

Activez ces paramètres lorsque l'une des conditions suivantes est vraie :

- Votre origine renvoie des objets compressés Gzip lorsque les utilisateurs les prennent en charge (les demandes contiennent l'en-tête `Accept-Encoding` HTTP avec `gzip` comme valeur). Dans ce cas, utilisez le paramètre activé par Gzip (défini `EnableAcceptEncodingGzip` sur `true` dans l' CloudFront API, AWS SDKs AWS CLI, ou CloudFormation).
- Votre origine renvoie des objets compressés Brotli lorsque les utilisateurs les prennent en charge (les demandes contiennent l'en-tête `Accept-Encoding` HTTP avec `br` comme valeur). Dans ce cas, utilisez le paramètre activé par Brotli (défini sur `EnableAcceptEncodingBrotli` `true` dans l' CloudFront API, AWS SDKs AWS CLI, ou CloudFormation).
- Le comportement de cache auquel cette stratégie de cache est attachée est configuré avec la compression CloudFront. Dans ce cas, vous pouvez activer la mise en cache pour Gzip ou Brotli, ou les deux. Lorsque CloudFront la compression est activée, l'activation de la mise en cache pour les deux formats peut contribuer à réduire les coûts de transfert de données vers Internet.

> **Note**
>
> Si vous activez la mise en cache pour l'un de ces formats de compression ou pour les deux, n'incluez pas l'`Accept-Encoding`en-tête dans une politique de demande d'origine associée au même comportement de cache. CloudFront inclut toujours cet en-tête dans les demandes d'origine lorsque la mise en cache est activée pour l'un ou l'autre de ces formats. L'inclusion `Accept-Encoding` dans une politique de demande d'origine n'a donc aucun effet.

Si votre serveur d'origine ne renvoie pas d'objets compressés Gzip ou Brotli, ou si le comportement du cache n'est pas configuré avec la CloudFront compression, n'activez pas la

mise en cache pour les objets compressés. Si vous le faites, cela peut entraîner une diminution du taux d'accès au cache.

Ce qui suit explique comment ces paramètres affectent une CloudFront distribution. Tous les scénarios suivants supposent que la demande de l'utilisateur inclut l'en-tête `Accept-Encoding`. Lorsque la demande du visualiseur n'inclut pas l'`Accept-Encoding`en-tête, CloudFront ne l'inclut pas dans la clé de cache et ne l'inclut pas dans la demande d'origine correspondante.

Lorsque la mise en cache des objets compressés est activée pour les deux formats de compression

Si le visualiseur prend en charge à la fois Gzip et Brotli, c'est-à-dire si les `br` valeurs `gzip` et figurent toutes deux dans l'`Accept-Encoding`en-tête de la demande du visualiseur, effectue les opérations suivantes : CloudFront

- Normalise l'en-tête sur `Accept-Encoding: br,gzip` et inclut l'en-tête normalisé dans la clé de cache. La clé de cache n'inclut pas d'autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.
- Si le cache contient un objet compressé Brotli ou Gzip qui correspond à la demande et n'a pas expiré, cet emplacement renvoie l'objet à l'utilisateur.
- Si le cache de l'emplacement périphérique ne contient aucun objet compressé Brotli ou Gzip correspondant à la demande et n'ayant pas expiré, CloudFront inclut l'en-tête normalisé (`Accept-Encoding: br,gzip`) dans la demande d'origine correspondante. La demande d'origine n'inclut pas les autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.

Si le visualiseur prend en charge un format de compression mais pas l'autre (par exemple, s'il s'`gzip`agit d'une valeur dans l'`Accept-Encoding`en-tête de la demande du lecteur mais ne l'`br`est pas), CloudFront effectue les opérations suivantes :

- Normalise l'en-tête sur `Accept-Encoding: gzip` et inclut l'en-tête normalisé dans la clé de cache. La clé de cache n'inclut pas d'autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.
- Si le cache contient un objet compressé Gzip qui correspond à la demande et n'a pas expiré, l'emplacement périphérique renvoie l'objet à l'utilisateur.
- Si le cache de l'emplacement périphérique ne contient aucun objet compressé Gzip correspondant à la demande et n'ayant pas expiré, CloudFront inclut l'en-tête normalisé (`Accept-Encoding: gzip`) dans la demande d'origine correspondante. La demande

d’origine n’inclut pas les autres valeurs qui se trouvaient dans l’en-tête `Accept-Encoding` envoyé par l’utilisateur.

Pour comprendre ce qui CloudFront se passe si le lecteur prend en charge Brotli mais pas Gzip, remplacez les deux formats de compression dans l'exemple précédent.

Si le lecteur ne prend pas en charge Brotli ou GZIP, c'est-à-dire que l'`Accept-Encoding`en-tête de la demande du lecteur ne contient pas de valeurs ou ne contient `br` pas de valeurs : `gzip` CloudFront

- N’inclut pas l’en-tête `Accept-Encoding` dans la clé de cache.
- Inclut `Accept-Encoding: identity` dans la demande d’origine correspondante. La demande d’origine n’inclut pas les autres valeurs qui se trouvaient dans l’en-tête `Accept-Encoding` envoyé par l’utilisateur.

Lorsque la mise en cache des objets compressés est activée pour un format de compression, mais pas pour l'autre

Si le visualiseur prend en charge le format pour lequel la mise en cache est activée, par exemple, si la mise en cache des objets compressés est activée pour Gzip et que le visualiseur prend en charge Gzip (`gzip`c'est l'une des valeurs de l'`Accept-Encoding`en-tête de la demande du lecteur), procède comme suit : CloudFront

- Normalise l'en-tête sur `Accept-Encoding: gzip` et inclut l'en-tête normalisé dans la clé de cache.
- Si le cache contient un objet compressé Gzip qui correspond à la demande et n’a pas expiré, l’emplacement périphérique renvoie l’objet à l’utilisateur.
- Si le cache de l'emplacement périphérique ne contient aucun objet compressé Gzip correspondant à la demande et n'ayant pas expiré, CloudFront inclut l'en-tête normalisé (`Accept-Encoding: gzip`) dans la demande d'origine correspondante. La demande d’origine n’inclut pas les autres valeurs qui se trouvaient dans l’en-tête `Accept-Encoding` envoyé par l’utilisateur.

Ce comportement est le même lorsque l'utilisateur prend en charge Gzip et Brotli (l'en-tête `Accept-Encoding` de la demande de l'utilisateur inclut les deux `gzip` et `br` comme valeurs), car dans ce scénario, la mise en cache des objets compressés pour Brotli n'est pas activée.

Pour comprendre ce qui CloudFront se passe si la mise en cache des objets compressés est activée pour Brotli mais pas pour Gzip, remplacez les deux formats de compression dans l'exemple précédent.

Si le lecteur ne prend pas en charge le format de compression pour lequel la mise en cache est activée (l'`Accept-Encoding`en-tête de la demande du lecteur ne contient pas la valeur de ce format), CloudFront :

- N'inclut pas l'en-tête `Accept-Encoding` dans la clé de cache.
- Inclut `Accept-Encoding: identity` dans la demande d'origine correspondante. La demande d'origine n'inclut pas les autres valeurs qui se trouvaient dans l'en-tête `Accept-Encoding` envoyé par l'utilisateur.

Lorsque la mise en cache des objets compressés est désactivée pour les deux formats de compression

Lorsque la mise en cache des objets compressés est désactivée pour les deux formats de compression, CloudFront traite l'`Accept-Encoding`en-tête de la même manière que tout autre en-tête HTTP dans la demande du visualiseur. Par défaut, il n'est pas inclus dans la clé de cache et il n'est pas inclus dans les demandes de l'origine. Vous pouvez l'inclure dans la liste d'autorisation des en-têtes dans une politique de cache ou une politique de demande d'origine comme tout autre en-tête HTTP.

Création de politiques de cache

Vous pouvez utiliser une politique de cache pour améliorer votre taux d'accès au cache en contrôlant les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) incluses dans la clé de cache. Vous pouvez créer une politique de cache dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Après avoir créé une stratégie de cache, vous l'associez à un ou plusieurs comportements de cache dans une distribution CloudFront .

Console

Pour créer une politique de cache (console)

1. Connectez-vous à la page Politiques Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home?#/policies.
2. Choisissez Créer une politique de cache.
3. Choisissez le paramètre souhaité pour cette politique de cache. Pour plus d'informations, consultez Compréhension des politiques de cache.

4. Lorsque vous avez terminé, choisissez Create (Créer).

Après avoir créé une politique de cache, vous pouvez l'attacher à un comportement de cache.

Pour attacher une politique de cache à une distribution existante (console)

1. Ouvrez la page Distributions dans la console CloudFront à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Choisissez la distribution à mettre à jour, puis choisissez l'onglet Comportements.
3. Choisissez le comportement du cache à mettre à jour, puis choisissez Modifier.

   Ou, pour créer un nouveau comportement de cache, choisissez Create behavior (Créer un comportement).
4. Dans la section Clé de cache et demandes d'origine, assurez-vous que l'option Politique de cache et politique de demande d'origine est sélectionnée.
5. Pour Cache policy (Politique de cache), choisissez la politique de cache à attacher à ce comportement de cache.
6. Choisissez Save changes (Enregistrer les modifications) en bas de la page.

Pour attacher une politique de cache à une nouvelle distribution (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Dans la section Clé de cache et demandes d'origine, assurez-vous que l'option Politique de cache et politique de demande d'origine est sélectionnée.
4. Pour Cache policy (Politique de cache), choisissez la politique de cache à attacher au comportement de cache par défaut de cette distribution.
5. Choisissez les paramètres souhaités pour l'origine, le comportement de cache par défaut et les autres paramètres de distribution. Pour plus d'informations, consultez Référence de tous les paramètres de distribution.
6. Lorsque vous avez terminé, choisissez Create distribution (Créer une distribution).

CLI

Pour créer une politique de cache avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-cache-policy commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une politique de cache (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `cache-policy.yaml` qui contient tous les paramètres d'entrée de la commande create-cache-policy.

   ```
   aws cloudfront create-cache-policy --generate-cli-skeleton yaml-input > cache-policy.yaml
   ```

2. Ouvrez le fichier nommé `cache-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de politique de cache que vous souhaitez, puis enregistrez le fichier. Vous pouvez supprimer des champs facultatifs du fichier, mais ne supprimez pas les champs obligatoires.

   Pour plus d'informations sur les paramètres de politique de cache, consultez Compréhension des politiques de cache.

3. Utilisez la commande suivante pour créer la politique de cache à l'aide des paramètres d'entrée du fichier `cache-policy.yaml`.

   ```
   aws cloudfront create-cache-policy --cli-input-yaml file://cache-policy.yaml
   ```

   Notez la valeur `Id` dans la sortie de la commande. Il s'agit de l'ID de politique de cache, dont vous avez besoin pour associer la politique de cache au comportement de cache d'une CloudFront distribution.

Pour attacher une politique de cache à une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes à chaque comportement de cache que vous mettez à jour pour utiliser une politique de cache.

   - Dans le comportement du cache, ajoutez un champ nommé `CachePolicyId`. Pour la valeur du champ, utilisez l'ID de politique de cache que vous avez noté après la création de la politique.
   - Supprimez les champs `MinTTL`, `MaxTTL`, `DefaultTTL` et `ForwardedValues` du comportement du cache. Ces paramètres sont spécifiés dans la politique de cache, de sorte que vous ne pouvez pas inclure ces champs et une politique de cache dans le même comportement de cache.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la politique de cache. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Pour attacher une politique de cache à une nouvelle distribution (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `distribution.yaml` qui contient tous les paramètres d’entrée de la commande create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Ouvrez le fichier nommé `distribution.yaml` que vous venez de créer. Dans le comportement de cache par défaut, dans le champ `CachePolicyId`, entrez l'ID de politique

de cache que vous avez noté après la création de la politique. Poursuivez la modification du fichier pour spécifier les paramètres de distribution souhaité, puis enregistrez le fichier lorsque vous avez terminé.

Pour plus d'informations sur les paramètres de distribution, consultez Référence de tous les paramètres de distribution.

3. Utilisez la commande suivante pour créer la distribution à l'aide des paramètres d'entrée du fichier `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Pour créer une politique de cache avec l' CloudFront API, utilisez CreateCachePolicy. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez Compréhension des politiques de cache la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une politique de cache, vous pouvez l'attacher à un comportement de cache, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de la politique de cache dans le champ `CachePolicyId`, à l'intérieur d'un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence de tous les paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Utilisation des politiques de cache gérées

CloudFront fournit un ensemble de politiques de cache gérées que vous pouvez associer à tous les comportements de cache de votre distribution. Avec une stratégie de cache gérée, vous n'avez pas besoin d'écrire ou de gérer votre propre stratégie de cache. Les stratégies gérées utilisent des paramètres optimisés pour des cas d'utilisation spécifiques.

Pour utiliser une stratégie de cache gérée, vous l'attachez à un comportement de cache dans votre distribution. Le processus est le même que lorsque vous créez une stratégie de cache, mais au lieu d'en créer une nouvelle, vous n'avez qu'à attacher l'une des stratégies de cache gérées. Vous joignez la politique soit par son nom (avec la console), soit par son identifiant (avec le AWS CLI ou SDKs). Les noms et IDs les noms sont répertoriés dans la section suivante.

Pour de plus amples informations, veuillez consulter Création de politiques de cache.

Les rubriques suivantes décrivent les stratégies de cache gérées que vous pouvez utiliser.

Rubriques

- Amplify
- CachingDisabled
- CachingOptimized
- CachingOptimizedForUncompressedObjects
- Élémentaire- MediaPackage
- UseOriginCacheControlHeaders
- UseOriginCacheControlHeaders-QueryStrings

Amplify

Afficher cette politique dans la CloudFront console

Cette stratégie est conçue pour être utilisée avec une origine qui est une appli web AWS Amplify.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

```
2e54312d-136d-493c-8eb9-b001f22f67d2
```

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 2 secondes
- Maximum TTL (Durée de vie maximale) : 600 secondes (10 minutes)
- Default TTL (Durée de vie par défaut) : 2 secondes
- En-têtes inclus dans la clé de cache :
  - `Authorization`
  - `CloudFront-Viewer-Country`
  - `Host`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé. Pour plus d'informations, consultez Prise en charge de la compression.
- Cookies included in cache key (Cookies inclus dans la clé de cache) : tous les cookies sont inclus.
- Query strings included in cache key (Chaînes de requête incluses dans la clé de cache) : toutes les chaînes de requête sont incluses.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, consultez Prise en charge de la compression.

> **Warning**
>
> Comme cette politique a un TTL minimum supérieur à 0, le contenu CloudFront sera mis en cache pendant au moins la durée spécifiée dans le TTL minimum de la politique de cache, même si les `private` directives `Cache-Control: no-cacheno-store`, ou sont présentes dans les en-têtes d'origine.

AWS Amplify Politiques de cache d'hébergement

Amplify utilise les politiques de cache gérées suivantes pour optimiser la configuration de cache par défaut pour les applications des clients :

- Amplify-Default
- Amplifier- DefaultNoCookies
- Amplifier- ImageOptimization
- Amplifier- StaticContent

> **Note**
>
> Ces politiques ne sont utilisées que par Amplify. Nous vous déconseillons d'utiliser ces politiques pour vos distributions.

Pour plus d'informations sur la gestion de la configuration du cache pour votre application hébergée avec Amplify, consultez Gestion de la configuration de cache dans le Guide de l'utilisateur Amplify Hosting.

CachingDisabled

Afficher cette politique dans la CloudFront console

Cette stratégie désactive la mise en cache. Cette stratégie est utile pour le contenu dynamique et pour les demandes qui ne peuvent pas être mises en cache.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

```
4135ea2d-6df8-44a3-9df3-4b5a84be39ad
```

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 0 seconde
- Default TTL (Durée de vie par défaut) : 0 seconde
- Headers included in the cache key (En-têtes inclus dans la clé de cache) : aucun
- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune
- Paramètre des objets compressés du cache : Désactivé

CachingOptimized

Afficher cette politique dans la CloudFront console

Cette politique est conçue pour optimiser l'efficacité du cache en minimisant les valeurs CloudFront incluses dans la clé de cache. CloudFront n'inclut aucune chaîne de requête ni aucun cookie dans la clé de cache et inclut uniquement l'`Accept-Encoding`en-tête normalisé. Cela permet CloudFront de mettre en cache séparément les objets aux formats de compression Gzip et Brotli lorsque l'origine les renvoie ou lorsque la compression des CloudFront bords est activée.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`658327ea-f89d-4fab-a63d-7e88639e58f6`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 1 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours).
- Default TTL (Durée de vie par défaut) : 86 400 secondes (24 heures).
- Headers included in the cache key (En-têtes inclus dans la clé de cache) : aucun n'est explicitement inclus. L'en-tête `Accept-Encoding` normalisé est inclus car le paramètre des objets compressés du cache est activé. Pour plus d'informations, consultez Prise en charge de la compression.
- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun.
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, consultez Prise en charge de la compression.

> **Warning**
>
> Comme cette politique a un TTL minimum supérieur à 0, le contenu CloudFront sera mis en cache pendant au moins la durée spécifiée dans le TTL minimum de la politique de cache, même si les `private` directives `Cache-Control: no-cache` `no-store`, ou sont présentes dans les en-têtes d'origine.

CachingOptimizedForUncompressedObjects

Afficher cette politique dans la CloudFront console

Cette stratégie est conçue pour optimiser l'efficacité du cache en minimisant les valeurs incluses dans la clé de cache. Aucune chaîne de requête, aucun en-tête ou cookie ne sont inclus. Cette stratégie est identique à la précédente, mais elle désactive le paramètre des objets compressés du cache.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`b2884449-e4de-46a7-ac36-70bc7f1ddd6d`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 1 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 86 400 secondes (24 heures)
- Headers included in the cache key (En-têtes inclus dans la clé de cache) : aucun
- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune
- Paramètre des objets compressés du cache : Désactivé

> **Warning**
>
> Comme cette politique a un TTL minimum supérieur à 0, le contenu CloudFront sera mis en cache pendant au moins la durée spécifiée dans le TTL minimum de la politique de cache, même si les `private` directives `Cache-Control: no-cache` `no-store`, ou sont présentes dans les en-têtes d'origine.

Élémentaire- MediaPackage

Afficher cette politique dans la CloudFront console

Cette stratégie est conçue pour être utilisée avec une origine qui est un point de terminaison AWS Elemental MediaPackage .

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`08627262-05a9-4f76-9ded-b50ca2e3a84f`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 86 400 secondes (24 heures)
- Headers included in the cache key (En-têtes inclus dans la clé de cache) :
  - `Origin`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé pour Gzip. Pour plus d'informations, consultez Prise en charge de la compression.
- Cookies included in the cache key (Cookies inclus dans la clé de cache) : aucun
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) :
  - `aws.manifestfilter`
  - `start`
  - `end`
  - `m`
- Cache compressed objects setting (Paramètre des objets compressés du cache) : activé pour Gzip. Pour plus d'informations, consultez Prise en charge de la compression.

UseOriginCacheControlHeaders

Afficher cette politique dans la CloudFront console

Cette politique est conçue pour être utilisée avec une origine qui renvoie des en-têtes de réponse HTTP `Cache-Control` et ne diffuse pas de contenu différent en fonction des valeurs présentes dans la chaîne de requête. Si votre origine sert un contenu différent en fonction des valeurs présentes dans la chaîne de requête, envisagez d'utiliser UseOriginCacheControlHeaders-QueryStrings.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`83da9c7e-98b4-4e11-a168-04f0df8e2c65`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 0 seconde
- Headers included in the cache key (En-têtes inclus dans la clé de cache) :
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé. Pour plus d'informations, consultez Prise en charge de la compression.
- Cookies inclus dans la clé de cache : tous les cookies sont inclus.
- Query strings included in the cache key (Chaînes de requête incluses dans la clé de cache) : aucune.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, consultez Prise en charge de la compression.

UseOriginCacheControlHeaders-QueryStrings

Afficher cette politique dans la CloudFront console

Cette politique est conçue pour être utilisée avec une origine qui renvoie des en-têtes de réponse HTTP `Cache-Control` et diffuse un contenu différent en fonction des valeurs présentes dans la chaîne de requête. Si votre origine ne diffuse pas de contenu différent en fonction des valeurs présentes dans la chaîne de requête, envisagez d'utiliser UseOriginCacheControlHeaders.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`4cc15a8a-d715-48a4-82b8-cc0b614638fe`

Cette stratégie possède les paramètres suivants :

- Minimum TTL (Durée de vie minimale) : 0 seconde
- Maximum TTL (Durée de vie maximale) : 31 536 000 secondes (365 jours)
- Default TTL (Durée de vie par défaut) : 0 seconde
- Headers included in the cache key (En-têtes inclus dans la clé de cache) :
  - `Host`
  - `Origin`
  - `X-HTTP-Method-Override`
  - `X-HTTP-Method`
  - `X-Method-Override`

  L'en-tête `Accept-Encoding` normalisé est également inclus, car le paramètre des objets compressés du cache est activé. Pour plus d'informations, consultez Prise en charge de la compression.
- Cookies inclus dans la clé de cache : tous les cookies sont inclus.
- Chaînes de requête incluses dans la clé de cache : toutes les chaînes de requête sont incluses.
- Paramètre des objets compressés du cache : activé. Pour plus d'informations, consultez Prise en charge de la compression.

Comprendre la clé de cache

La clé de cache détermine si une requête de l'utilisateur adressée à un emplacement CloudFront périphérique entraîne un accès au cache. La clé de cache est l'identifiant unique d'un objet dans le cache. Chaque objet du cache possède une clé de cache unique.

Un accès au cache se produit lorsqu'une demande d'utilisateur génère la même clé de cache qu'une requête précédente, et que l'objet de cette clé de cache est dans le cache de l'emplacement périphérique et valide. En cas d'accès au cache, l'objet demandé est diffusé au spectateur depuis un emplacement CloudFront périphérique, ce qui présente les avantages suivants :

- Réduction de la charge sur votre serveur d'origine
- Latence réduite pour l'utilisateur

Vous pouvez obtenir de meilleures performances à partir de votre site Web ou de votre application lorsque vous avez un taux d'accès au cache plus élevé (une proportion plus élevée de requêtes

de visionneuse entraînant un accès au cache). Une façon d'améliorer votre taux d'accès du cache est d'inclure uniquement les valeurs minimales nécessaires dans la clé de cache. Pour plus d'informations, consultez les sections suivantes.

Vous pouvez modifier les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) dans la clé de cache à l'aide d'une stratégie de cache. (Vous pouvez également modifier la clé de cache à l'aide d'un Lambda @Edgefunction ou d'une CloudFront fonction sur une demande de visualisation.) Avant de modifier la clé de cache, il est important de comprendre comment votre application est conçue et quand et comment elle peut servir différentes réponses en fonction des caractéristiques de la requête de la visionneuse. Lorsqu'une valeur dans la demande de visionneuse détermine la réponse renvoyée par votre origine, vous devez inclure cette valeur dans la clé de cache. Mais si vous incluez une valeur dans la clé de cache qui n'affecte pas la réponse renvoyée par votre origine, vous risquez de mettre en cache des objets en double.

Clé de cache par défaut

Par défaut, la clé de cache d'une CloudFront distribution inclut les informations suivantes :

- Le nom de domaine de la CloudFront distribution (par exemple, d111111abcdef8.cloudfront.net)
- Chemin d'URL de l'objet demandé (par exemple, `/content/stories/example-story.html`)

> **Note**
>
> La méthode `OPTIONS` est incluse dans la clé de cache pour les demandes `OPTIONS`. Cela signifie que les réponses aux demandes `OPTIONS` sont mises en cache séparément des réponses aux demandes `GET` et `HEAD`.

Les autres valeurs de la demande de visionneuse ne sont pas incluses dans la clé de cache, par défaut. Examinez la requête HTTP suivante provenant d'un navigateur Web.

```
            GET /content/stories/example-story.html?ref=0123abc&split-pages=false
HTTP/1.1
            Host: d111111abcdef8.cloudfront.net
            User-Agent: Mozilla/5.0 Gecko/20100101 Firefox/68.0
            Accept: text/html,*/*
            Accept-Language: en-US,en
            Cookie: session_id=01234abcd
```

```
            Referer: https://news.example.com/
```

Lorsqu'une demande d'utilisateur, telle que cet exemple, arrive dans un emplacement CloudFront périphérique, CloudFront utilise la clé de cache pour déterminer s'il y a un accès au cache. Par défaut, seuls les composants suivants de la demande sont inclus dans la clé de cache : `/content/stories/example-story.html` et `d111111abcdef8.cloudfront.net`. Si l'objet demandé ne se trouve pas dans le cache (erreur de cache), CloudFront envoie une demande à l'origine pour obtenir l'objet. Après avoir récupéré l'objet, le CloudFront renvoie au visualiseur et le stocke dans le cache de l'emplacement périphérique.

Lorsque CloudFront reçoit une autre demande pour le même objet, telle que déterminée par la clé de cache CloudFront , transmet immédiatement l'objet mis en cache au spectateur, sans envoyer de demande à l'origine. Prenons l'exemple de la demande HTTP suivante qui vient après la demande précédente.

```
            GET /content/stories/example-story.html?ref=xyz987&split-pages=true
HTTP/1.1
            Host: d111111abcdef8.cloudfront.net
            User-Agent: Mozilla/5.0 AppleWebKit/537.36 Chrome/83.0.4103.116
            Accept: text/html,*/*
            Accept-Language: en-US,en
            Cookie: session_id=wxyz9876
            Referer: https://rss.news.example.net/
```

Cette demande concerne le même objet que la demande précédente, mais elle est différente de la demande précédente. Il a une chaîne de requête URL différente, différents en-têtes `User-Agent` et `Referer` et un cookie `session_id` différent. Cependant, aucune de ces valeurs ne fait partie de la clé de cache par défaut, de sorte que cette deuxième demande entraîne un accès au cache.

Personnalisation de la clé de cache

Dans certains cas, vous pouvez inclure plus d'informations dans la clé de cache, même si cela peut entraîner moins de visites de cache. Vous spécifiez les éléments à inclure dans la clé de cache à l'aide d'une stratégie de cache.

Par exemple, si votre serveur d'origine utilise l'en-tête HTTP `Accept-Language` dans les demandes de l'utilisateur pour renvoyer un contenu différent en fonction de la langue de l'utilisateur, vous

pouvez inclure cet en-tête dans la clé de cache. Dans ce cas, CloudFront utilise cet en-tête pour déterminer les accès au cache et inclut l'en-tête dans les requêtes d'origine (requêtes CloudFront envoyées à l'origine en cas d'échec de cache).

L'une des conséquences potentielles de l'inclusion de valeurs supplémentaires dans la clé de cache est que des objets dupliqués CloudFront pourraient être mis en cache en raison de la variation qui peut survenir dans les demandes des utilisateurs. Par exemple, les utilisateurs peuvent envoyer l'une des valeurs suivantes pour l'en-tête `Accept-Language` :

- `en-US,en`
- `en,en-US`
- `en-US, en`
- `en-US`

Toutes ces différentes valeurs indiquent que la langue de l'utilisateur est l'anglais, mais la variation peut CloudFront entraîner la mise en cache du même objet plusieurs fois. Cela peut réduire les accès au cache et augmenter le nombre de demandes d'origine. Vous pouvez éviter cette duplication en n'incluant pas l'en-tête `Accept-Language` dans la clé de cache et en configurant votre site Web ou votre application de manière à utiliser différentes URL pour le contenu dans différentes langues (par exemple, `/en-US/content/stories/example-story.html`).

Pour toute valeur donnée que vous avez l'intention d'inclure dans la clé de cache, vous devez vous assurer de comprendre combien de variations différentes de cette valeur peuvent apparaître dans les demandes de l'utilisateur. Pour certaines valeurs de demande, il est rarement logique de les inclure dans la clé de cache. Par exemple, l'en-tête `User-Agent` peut avoir des milliers de variations uniques, de sorte que ce n'est généralement pas un bon candidat à inclure dans la clé de cache. Les cookies qui ont des valeurs spécifiques à l'utilisateur ou à la session et qui sont uniques sur des milliers (voire des millions) de demandes ne sont pas non plus de bons candidats pour l'inclusion dans la clé de cache. Si vous incluez ces valeurs dans la clé de cache, chaque variation unique entraîne une autre copie de l'objet dans le cache. Si ces copies de l'objet ne sont pas uniques, ou si vous vous retrouvez avec un nombre si important d'objets légèrement différents que chaque objet ne reçoit qu'un petit nombre de visites de cache, vous pouvez envisager une approche différente. Vous pouvez exclure ces valeurs hautement variables de la clé de cache ou marquer des objets comme ne pouvant pas être mis en cache.

Faites preuve de prudence lors de la personnalisation de la clé de cache. Parfois, c'est souhaitable, mais cela peut avoir des conséquences inattendues telles que la mise en cache des objets en

double, la réduction du taux d'accès du cache et l'augmentation du nombre de demandes d'origine. Parfois, votre site Web ou application d'origine a besoin de certaines valeurs provenant des demandes des internautes à des fins d'analyse, de télémétrie ou autres, mais ces valeurs ne modifient pas l'objet renvoyé par l'origine. Dans ce cas, utilisez une politique de demande d'origine pour inclure ces valeurs dans les demandes d'origine, mais pas dans la clé de cache.

Contrôle des demandes d’origine à l’aide d’une stratégie

Lorsqu'une demande d'affichage CloudFront entraîne un échec du cache (l'objet demandé n'est pas mis en cache à l'emplacement périphérique), CloudFront envoie une demande à l'origine pour récupérer l'objet. C'est ce qu'on appelle une demande d'origine. La demande d'origine inclut toujours les informations suivantes provenant de la demande de l'utilisateur :

- Le chemin d'URL (le chemin uniquement, sans les chaînes de requête d'URL ou le nom de domaine)
- Le corps de la requête (s'il y en a un)
- Les en-têtes HTTP qui CloudFront sont automatiquement inclus dans chaque demande d'origine, notamment `HostUser-Agent`, et `X-Amz-Cf-Id`

D'autres informations provenant de la demande de l'utilisateur, telles que les chaînes de requête URL, les en-têtes HTTP et les cookies, ne sont pas incluses dans la demande d'origine par défaut. (Exception : avec les anciens paramètres de cache CloudFront , les en-têtes sont transférés par défaut vers votre origine.) Toutefois, vous pouvez demander à recevoir certaines de ces autres informations à l’origine, par exemple pour collecter des données à des fins d’analyse ou de télémétrie. Vous pouvez utiliser une stratégie de demande d'origine pour contrôler les informations incluses dans une demande d'origine.

Les stratégies de demande d'origine sont séparées des stratégies de cache, qui contrôlent la clé de cache. Ainsi, vous pouvez recevoir des informations supplémentaires à l’origine et maintenir un bon taux d’accès au cache (proportion de demandes de l’utilisateur qui entraînent un accès au cache). Pour ce faire, contrôlez séparément quelles informations sont incluses dans les demandes d'origine (à l'aide de la stratégie de demande d'origine) et celles qui sont incluses dans la clé de cache (à l'aide de la stratégie de cache).

Bien que les deux types de stratégie soient distincts, elles sont liées. Toutes les chaînes de requête URL, les en-têtes HTTP et les cookies que vous incluez dans la clé de cache (à l'aide d'une stratégie de cache) sont automatiquement inclus dans les requêtes d'origine. Utilisez la stratégie de demande d'origine pour spécifier les informations que vous souhaitez inclure dans les demandes d'origine, mais pas dans la clé de cache. Tout comme une politique de cache, vous associez une politique de demande d'origine à un ou plusieurs comportements de cache dans une CloudFront distribution.

Vous pouvez également utiliser une stratégie de demande d'origine pour ajouter des en-têtes HTTP supplémentaires à une demande d'origine qui n'étaient pas inclus dans la demande de l'utilisateur.

Ces en-têtes supplémentaires sont ajoutés CloudFront avant l'envoi de la demande d'origine, avec des valeurs d'en-tête qui sont déterminées automatiquement en fonction de la demande du spectateur. Pour de plus amples informations, veuillez consulter the section called “Ajouter des en-têtes de CloudFront demande”.

Rubriques

- Compréhension des stratégies de demande d’origine
- Création de stratégies de demande d’origine
- Utilisation des stratégies de demande d’origine gérées
- Ajouter des en-têtes de CloudFront demande
- Comprendre comment les politiques de demande d’origine et les politiques de cache fonctionnent ensemble

Compréhension des stratégies de demande d’origine

CloudFront fournit des politiques de demande d'origine prédéfinies, appelées politiques gérées, pour les cas d'utilisation courants. Vous pouvez utiliser ces stratégies gérées ou créer votre propre stratégie de demande d'origine spécifique à vos besoins. Pour plus d’informations sur les stratégies gérées, consultez Utilisation des stratégies de demande d’origine gérées.

Une stratégie de demande d'origine contient les paramètres suivants, qui sont classés en informations de stratégie et en paramètres de demande d'origine.

Informations sur les stratégies

Nom

Nom permettant d'identifier la stratégie de demande d'origine. Dans la console, vous utilisez le nom pour attacher la stratégie de demande d'origine à un comportement de cache.

Description

Commentaire décrivant la stratégie de demande de l'origine. Facultative.

Paramètres de la demande d'origine

Les paramètres de demande d'origine spécifient les valeurs des demandes du lecteur qui sont incluses dans les demandes CloudFront envoyées à l'origine (appelées demandes d'origine). Les

valeurs peuvent inclure des chaînes de requête URL, des en-têtes HTTP et des cookies. Les valeurs que vous spécifiez sont incluses dans les demandes d'origine, mais ne sont pas incluses dans la clé de cache. Pour plus d'informations sur le contrôle de la clé cache, consultez Contrôle de la clé de cache à l'aide d'une politique.

En-têtes

Les en-têtes HTTP dans les demandes du lecteur, CloudFront y compris dans les demandes d'origine. Pour les en-têtes, vous pouvez choisir l'un des paramètres suivants :

- Aucun : les en-têtes HTTP des demandes de l'utilisateur ne sont pas inclus dans les demandes d'origine.
- Tous les en-têtes de l'utilisateur : tous les en-têtes HTTP des demandes de l'utilisateur sont inclus dans les demandes d'origine.
- Tous les en-têtes du visualiseur et les CloudFront en-têtes suivants : tous les en-têtes HTTP des requêtes du visualiseur sont inclus dans les requêtes d'origine. En outre, vous spécifiez les CloudFront en-têtes que vous souhaitez ajouter aux demandes d'origine. Pour plus d'informations sur les CloudFront en-têtes, consultezthe section called "Ajouter des en-têtes de CloudFront demande".
- Include the following headers (Inclure les en-têtes suivants) : vous spécifiez quels en-têtes HTTP sont inclus dans les demandes d'origine.

  > **Note**
  >
  > Ne spécifiez pas un en-tête déjà inclus dans vos paramètres En-têtes personnalisés de l'origine. Pour de plus amples informations, veuillez consulter Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine.

- Tous les en-têtes de visionnage, à l'exception de – vous spécifiez les en-têtes HTTP qui ne sont pas inclus dans les demandes d'origine. Tous les autres en-têtes HTTP contenus dans les demandes de visionnage, à l'exception de ceux spécifiés, sont inclus.

Lorsque vous utilisez tous les en-têtes de visionneuse et les CloudFront en-têtes suivants, incluez les en-têtes suivants ou Tous les en-têtes de visionneuse sauf le paramètre, vous spécifiez les en-têtes HTTP uniquement par leur nom d'en-tête. CloudFront inclut l'en-tête complet, y compris sa valeur, dans les demandes d'origine.

> **Note**
>
> Lorsque vous utilisez le paramètre Tous les en-têtes du lecteur sauf pour supprimer l'`Host`en-tête du lecteur, vous ajoutez CloudFront un nouvel `Host` en-tête avec le nom de domaine de l'origine à la demande d'origine.

Cookies

Les cookies contenus dans les demandes des utilisateurs, CloudFront y compris dans les demandes d'origine. Pour les cookies, vous pouvez choisir l'un des paramètres suivants :

- Aucun : les cookies dans les demandes de l'utilisateur ne sont pas inclus dans les demandes d'origine.
- Tous : tous les cookies dans les demandes de l'utilisateur sont inclus dans les demandes d'origine.
- Inclure les cookies suivants – vous spécifiez quels cookies figurant dans les demandes de visionnage sont inclus dans les demandes d'origine.
- Tous les cookies sauf – vous spécifiez quels cookies figurant dans les demandes de visionnage ne sont pas inclus dans les demandes d'origine. Tous les autres cookies figurant dans les demandes de visionnage sont inclus.

Lorsque vous utilisez le paramètre Inclure les cookies suivants ou Tous les cookies sauf, vous spécifiez les cookies uniquement par leur nom. CloudFront inclut le cookie complet, y compris sa valeur, dans les demandes d'origine.

Chaînes de requête

Les chaînes de requête d'URL contenues dans les demandes du visualiseur, CloudFront y compris dans les demandes d'origine. Pour les chaînes de requête, vous pouvez choisir l'un des paramètres suivants :

- Aucun : les chaînes de requête dans les demandes de l'utilisateur ne sont pas incluses dans les demandes d'origine.
- Toutes : toutes les chaînes de requête dans les demandes de l'utilisateur sont incluses dans les demandes d'origine.
- Inclure les chaînes de requête suivantes – vous spécifiez quelles chaînes de requête figurant dans les demandes de visionnage sont incluses dans les demandes d'origine.

- Toutes les chaînes de requête sauf – vous spécifiez quelles chaînes de requête figurant dans les demandes de visionnage ne sont pas incluses dans les demandes d'origine. Toutes les autres chaînes de requête sont incluses.

Lorsque vous utilisez le paramètre Inclure les chaînes de requête suivantes ou Toutes les chaînes de requête sauf, vous spécifiez les chaînes de requête uniquement par leur nom. CloudFront inclut la chaîne de requête complète, y compris sa valeur, dans les demandes d'origine.

Création de stratégies de demande d’origine

Vous pouvez utiliser une politique de demande d'origine pour contrôler les valeurs (chaînes de requête URL, en-têtes HTTP et cookies) incluses dans les demandes CloudFront envoyées à votre origine. Vous pouvez créer une politique de demande d'origine dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Après avoir créé une politique de demande d'origine, vous l'associez à un ou plusieurs comportements de cache dans une CloudFront distribution.

Les stratégies de demande d'origine ne sont pas obligatoires. Lorsqu'un comportement de cache n'a pas de stratégie de demande d'origine attachée, la demande d'origine inclut toutes les valeurs spécifiées dans la stratégie de cache, mais rien de plus.

> **Note**
>
> Pour utiliser une stratégie de demande d'origine, le comportement de cache doit également utiliser une stratégie de cache. Vous ne pouvez pas utiliser de stratégie de demande d'origine dans un comportement de cache sans stratégie de cache.

Console

Pour créer une stratégie de demande d'origine (console)

1. Connectez-vous à la page Politiques Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home?#/policies.
2. Choisissez Origin request (Demande d'origine), puis Create origin request policy (Créer une stratégie de demande d'origine).

3. Choisissez le paramètre souhaité pour cette stratégie de demande d'origine. Pour plus d'informations, consultez Compréhension des stratégies de demande d’origine.
4. Lorsque vous avez terminé, choisissez Create (Créer).

Après avoir créé une stratégie de demande d'origine, vous pouvez l'attacher à un comportement de cache.

Pour attacher une stratégie de demande d'origine à une distribution existante (console)

1. Ouvrez la page Distributions dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Choisissez la distribution à mettre à jour, puis choisissez l'onglet Comportements.
3. Choisissez le comportement du cache à mettre à jour, puis choisissez Modifier.

   Ou, pour créer un nouveau comportement de cache, choisissez Create behavior (Créer un comportement).
4. Dans la section Clé de cache et demandes d’origine, assurez-vous que l’option Politique de cache et politique de demande d’origine est sélectionnée.
5. Pour Origin request policy (Stratégie de demande d'origine), choisissez la stratégie de demande d'origine à attacher à ce comportement de cache.
6. Choisissez Save changes (Enregistrer les modifications) en bas de la page.

Pour attacher une stratégie de demande d'origine à une nouvelle distribution (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Dans la section Clé de cache et demandes d’origine, assurez-vous que l’option Politique de cache et politique de demande d’origine est sélectionnée.
4. Pour Origin request policy (Stratégie de demande d'origine), choisissez la stratégie de demande d'origine à attacher au comportement de cache par défaut de cette distribution.
5. Choisissez les paramètres souhaités pour l’origine, le comportement de cache par défaut et les autres paramètres de distribution. Pour plus d'informations, consultez Référence de tous les paramètres de distribution.
6. Lorsque vous avez terminé, choisissez Create distribution (Créer une distribution).

CLI

Pour créer une politique de demande d'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-request-policy commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une stratégie de demande d'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-request-policy.yaml` qui contient tous les paramètres d'entrée de la commande create-origin-request-policy.

```
aws cloudfront create-origin-request-policy --generate-cli-skeleton yaml-input >
 origin-request-policy.yaml
```

2. Ouvrez le fichier nommé `origin-request-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de stratégie de demande d'origine que vous souhaitez, puis enregistrez le fichier. Vous pouvez supprimer des champs facultatifs du fichier, mais ne supprimez pas les champs obligatoires.

   Pour plus d'informations sur les paramètres de stratégie de demande d'origine, consultez Compréhension des stratégies de demande d'origine.

3. Utilisez la commande suivante pour créer la stratégie de demande d'origine à l'aide des paramètres d'entrée du fichier `origin-request-policy.yaml`.

```
aws cloudfront create-origin-request-policy --cli-input-yaml file://origin-
request-policy.yaml
```

   Notez la valeur `Id` dans la sortie de la commande. Il s'agit de l'ID de politique de demande d'origine, dont vous avez besoin pour associer la politique de demande d'origine au comportement du cache d'une CloudFront distribution.

Pour attacher une stratégie de demande d'origine à une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *distribution_ID* par l'ID de la distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes à chaque comportement de cache que vous mettez à jour pour utiliser une stratégie de demande d'origine.

   - Dans le comportement du cache, ajoutez un champ nommé `OriginRequestPolicyId`. Pour la valeur du champ, utilisez l'ID de stratégie de demande d'origine que vous avez noté après la création de la stratégie.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la stratégie de demande d'origine. Remplacez *distribution_ID* par l'ID de la distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Pour attacher une stratégie de demande d'origine à une nouvelle distribution (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `distribution.yaml` qui contient tous les paramètres d’entrée de la commande create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Ouvrez le fichier nommé `distribution.yaml` que vous venez de créer. Dans le comportement de cache par défaut, dans le champ `OriginRequestPolicyId`, entrez l'ID de stratégie de demande d'origine que vous avez noté après la création de la stratégie. Poursuivez la modification du fichier pour spécifier les paramètres de distribution souhaité, puis enregistrez le fichier lorsque vous avez terminé.

   Pour plus d'informations sur les paramètres de distribution, consultez Référence de tous les paramètres de distribution.

3. Utilisez la commande suivante pour créer la distribution à l'aide des paramètres d'entrée du fichier `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Pour créer une politique de demande d'origine avec l' CloudFront API, utilisez CreateOriginRequestPolicy. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez Compréhension des stratégies de demande d'origine la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une stratégie de demande d'origine, vous pouvez l'attacher à un comportement de cache, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de la stratégie de demande d'origine dans le champ `OriginRequestPolicyId`, à l'intérieur d'un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence de tous les paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Utilisation des stratégies de demande d’origine gérées

CloudFront fournit un ensemble de politiques de demande d'origine gérées que vous pouvez associer à tous les comportements de cache de votre distribution. Avec une stratégie de demande d'origine gérée, vous n'avez pas besoin d'écrire ou de gérer votre propre stratégie de demande d'origine. Les stratégies gérées utilisent des paramètres optimisés pour des cas d’utilisation spécifiques.

Pour utiliser une stratégie de demande d'origine gérée, vous l'attachez à un comportement de cache dans votre distribution. Le processus est le même que lorsque vous créez une stratégie de demande d'origine, mais au lieu d'en créer une nouvelle, vous n'avez qu'à attacher l'une des stratégies de demande d'origine gérée. Vous attachez la stratégie par nom (avec la console) ou par ID (avec le AWS CLI ou les kits SDK). Les noms et les identifiants sont répertoriés dans la section suivante.

Pour plus d’informations, consultez Création de stratégies de demande d’origine.

Les rubriques suivantes décrivent les stratégies de demande d’origine gérées que vous pouvez utiliser.

Rubriques

- AllViewer
- AllViewerAndCloudFrontHeaders-2022-06
- AllViewerExceptHostHeader
- CORS-CustomOrigin
- CORS-S3Origin
- Elemental-MediaTailor-PersonalizedManifests
- HostHeaderOnly
- UserAgentRefererHeaders

AllViewer

Afficher cette politique dans la CloudFront console

Cette politique inclut toutes les valeurs (en-têtes, cookies et chaînes de requête) dans la demande de visionnage.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`216adef6-5c7f-47e4-b989-5492eafa07d3`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine : Tous les en-têtes de la demande de l'utilisateur
- Cookies inclus dans les demandes d’origine : Tous
- Chaînes de requête incluses dans les demandes d’origine : Toutes

AllViewerAndCloudFrontHeaders-2022-06

Afficher cette politique dans la CloudFront console

Cette politique inclut toutes les valeurs (en-têtes, cookies et chaînes de requête) de la demande du lecteur, ainsi que tous les CloudFront en-têtes publiés jusqu'en juin 2022 (CloudFront les en-têtes publiés après juin 2022 ne sont pas inclus).

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`33f36d7e-f396-46d9-90e0-52428a34d9dc`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine : tous les en-têtes de la demande de visualisation, ainsi que les en-têtes suivants : CloudFront
  - `CloudFront-Forwarded-Proto`
  - `CloudFront-Is-Android-Viewer`
  - `CloudFront-Is-Desktop-Viewer`
  - `CloudFront-Is-IOS-Viewer`
  - `CloudFront-Is-Mobile-Viewer`
  - `CloudFront-Is-SmartTV-Viewer`
  - `CloudFront-Is-Tablet-Viewer`
  - `CloudFront-Viewer-Address`
  - `CloudFront-Viewer-ASN`
  - `CloudFront-Viewer-City`
  - `CloudFront-Viewer-Country`

- `CloudFront-Viewer-Country-Name`
- `CloudFront-Viewer-Country-Region`
- `CloudFront-Viewer-Country-Region-Name`
- `CloudFront-Viewer-Http-Version`
- `CloudFront-Viewer-Latitude`
- `CloudFront-Viewer-Longitude`
- `CloudFront-Viewer-Metro-Code`
- `CloudFront-Viewer-Postal-Code`
- `CloudFront-Viewer-Time-Zone`
- `CloudFront-Viewer-TLS`

- Cookies inclus dans les demandes d'origine : Tous
- Chaînes de requête incluses dans les demandes d'origine : Toutes

AllViewerExceptHostHeader

Afficher cette politique dans la CloudFront console

Cette politique n'inclut pas l'en-tête `Host` de la demande de visionnage, mais inclut toutes les autres valeurs (en-têtes, cookies et chaînes de requête) de la demande de visionnage.

Cette politique inclut également des en-têtes de CloudFront demande supplémentaires pour le protocole HTTP, la version HTTP, la version TLS, ainsi que tous les en-têtes de type d'appareil et de localisation du spectateur.

Cette politique est destinée à être utilisée avec Amazon API Gateway, l'URL des AWS Lambda fonctions et les origines des fonctions Web Lambda. Ces origines supposent que l'`Host`en-tête contienne le nom de domaine d'origine, et non le nom de domaine de la CloudFront distribution. Le transfert de l'en-tête `Host` de la demande de visionnage vers ces origines peut empêcher leur fonctionnement.

> **Note**
>
> Lorsque vous utilisez cette politique de gestion des demandes d'origine pour supprimer l'`Host`en-tête du lecteur, vous CloudFront ajoutez un nouvel `Host` en-tête avec le nom de domaine de l'origine à la demande d'origine.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`b689b0a8-53d0-40ab-baf2-68738e2966ac`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine : tous les en-têtes de la demande de visionnage à l'exception de l'en-tête `Host`
- Cookies inclus dans les demandes d’origine : Tous
- Chaînes de requête incluses dans les demandes d’origine : Toutes

CORS-CustomOrigin

Afficher cette politique dans la CloudFront console

Cette stratégie inclut l'en-tête qui active les demandes de partage de ressources croisées (CORS) lorsque l'origine est une origine personnalisée.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`59781a5b-3903-41f3-afcb-af62929ccde1`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `Origin`
- Cookies inclus dans les demandes d’origine : Aucun
- Chaînes de requête incluses dans les demandes d’origine : Aucune

CORS-S3Origin

Afficher cette politique dans la CloudFront console

Cette stratégie inclut les en-têtes qui activent les demandes de partage de ressources croisées (CORS) lorsque l'origine est un compartiment Amazon S3.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`88a5eaf4-2fd4-4709-b370-b4c650ea3fcf`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`
- Cookies inclus dans les demandes d’origine : Aucun
- Chaînes de requête incluses dans les demandes d’origine : Aucune

Elemental-MediaTailor-PersonalizedManifests

Afficher cette politique dans la CloudFront console

Cette stratégie est destinée à être utilisée avec une origine correspondant à un point de terminaison AWS Elemental MediaTailor .

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`775133bc-15f2-49f9-abea-afb2e0bf67d2`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `Origin`
  - `Access-Control-Request-Headers`
  - `Access-Control-Request-Method`
  - `User-Agent`
  - `X-Forwarded-For`
- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d’origine : Toutes

HostHeaderOnly

Afficher cette politique dans la CloudFront console

Cette stratégie inclut uniquement l'en-tête `Host` de la demande d'origine. Il n'inclut pas de chaînes de requête ni de cookies.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`bf0718e1-ba1e-49d1-88b1-f726733018ae`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine : hôte
- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d'origine : Aucune

UserAgentRefererHeaders

Afficher cette politique dans la CloudFront console

Cette stratégie inclut uniquement les en-têtes `User-Agent` et `Referer`. Il n'inclut pas de chaînes de requête ni de cookies.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`acba4595-bd28-49b8-b9fe-13317c0390fa`

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :
  - `User-Agent`
  - `Referer`
- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d'origine : Aucune

Ajouter des en-têtes de CloudFront demande

Vous pouvez configurer CloudFront pour ajouter des en-têtes HTTP spécifiques aux demandes CloudFront reçues des utilisateurs et transmises à votre fonction d'origine ou de périphérie. Les valeurs de ces en-têtes HTTP sont basées sur des caractéristiques de l'utilisateur ou sur la demande de l'utilisateur. Les en-têtes fournissent des informations sur le type d'appareil, l'adresse IP, l'emplacement géographique, le protocole de demande (HTTP ou HTTPS), la version HTTP, les détails de la connexion TLS, l'empreinte digitale et JA4 l'JA3 empreinte digitale du spectateur. Vous pouvez également configurer le comportement du cache de votre distribution pour transférer WebSocket les en-têtes. Pour de plus amples informations, veuillez consulter Utilisation WebSockets avec les CloudFront distributions.

Avec ces en-têtes, votre origine ou votre fonction périphérique peut recevoir des informations sur l'utilisateur sans avoir besoin d'écrire votre propre code pour déterminer ces informations. Si votre origine renvoie des réponses différentes en fonction des informations contenues dans ces en-têtes, vous pouvez les inclure dans la clé de cache afin que les réponses soient CloudFront mises en cache séparément. Par exemple, votre origine peut répondre avec du contenu dans une langue spécifique en fonction du pays dans lequel se trouve le visualiseur, ou avec du contenu adapté à un type d'appareil spécifique. Votre origine peut également écrire ces en-têtes dans des fichiers journaux, que vous pouvez utiliser pour déterminer où se trouvent vos spectateurs, quels types d'appareils ils se trouvent, et plus encore.

Pour inclure ces en-têtes dans la clé de cache, utilisez une politique de cache. Pour plus d'informations, consultez Contrôle de la clé de cache à l'aide d'une politique et the section called "Comprendre la clé de cache".

Pour recevoir des en-têtes à l'origine sans les inclure dans la clé de cache, utilisez une politique de demande de l'origine. Pour plus d'informations, consultez Contrôle des demandes d'origine à l'aide d'une stratégie.

Rubriques

- En-têtes de type d'appareil
- En-têtes de l'emplacement de l'utilisateur
- En-têtes permettant de déterminer la structure de l'en-tête de l'utilisateur
- En-têtes liés à TLS
- Autres CloudFront en-têtes

En-têtes de type d’appareil

Vous pouvez ajouter les en-têtes suivants pour déterminer le type d'appareil de l'utilisateur. En fonction de la valeur de l'`User-Agent`en-tête, CloudFront définit la valeur de ces en-têtes sur `true` ou`false`. Si un appareil entre dans plusieurs catégories, plusieurs valeurs peuvent être `true`. Par exemple, pour certaines tablettes, CloudFront définit à la fois `CloudFront-Is-Mobile-Viewer` et `CloudFront-Is-Tablet-Viewer` à`true`.

- `CloudFront-Is-Android-Viewer`— Réglé sur `true` quand CloudFront détermine que le spectateur est un appareil doté du système d'exploitation Android.
- `CloudFront-Is-Desktop-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le lecteur est un appareil de bureau.
- `CloudFront-Is-IOS-Viewer`— Réglé sur `true` quand CloudFront détermine que le spectateur est un appareil doté d'un système d'exploitation mobile Apple, tel qu'un iPhone, un iPod touch et certains iPad.
- `CloudFront-Is-Mobile-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le spectateur est un appareil mobile.
- `CloudFront-Is-SmartTV-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le téléspectateur est un téléviseur intelligent.
- `CloudFront-Is-Tablet-Viewer`— Réglé sur le `true` moment où CloudFront détermine que le lecteur est une tablette.

En-têtes de l’emplacement de l’utilisateur

Vous pouvez ajouter les en-têtes suivants pour déterminer la position du spectateur. CloudFront détermine les valeurs de ces en-têtes en fonction de l'adresse IP du spectateur. Pour les caractères non ASCII dans les valeurs de ces en-têtes, le CloudFront pourcentage code le caractère conformément à la section 1.2 de la RFC 3986.

- `CloudFront-Viewer-Address` : contient l'adresse IP de l'utilisateur et le port source de la demande. Par exemple, une valeur d'en-tête de `198.51.100.10:46532` signifie que l'adresse IP de l’utilisateur est 198.51.100.10 et que le port source de la demande est 46532.
- `CloudFront-Viewer-ASN` : contient le numéro de système autonome (ASN) de l'utilisateur.

> **Note**
>
> Vous pouvez ajouter `CloudFront-Viewer-Address` et `CloudFront-Viewer-ASN` dans une politique de demande d'origine, mais pas dans une politique de cache.

- `CloudFront-Viewer-Country` – Contient le code de pays à deux lettres du pays de l'utilisateur. Pour obtenir une liste des codes de pays, consultez ISO 3166-1 alpha-2.
- `CloudFront-Viewer-City` – Contient le nom de la ville de l'utilisateur.

Lorsque vous ajoutez les en-têtes suivants, CloudFront appliquez-les à toutes les demandes, à l'exception de celles qui proviennent du AWS réseau :

- `CloudFront-Viewer-Country-Name` – Contient le nom du pays de l'utilisateur.
- `CloudFront-Viewer-Country-Region` – Contient un code (jusqu'à trois caractères) représentant la région de l'utilisateur. La région est la subdivision de premier niveau (la plus large ou la moins spécifique) du code ISO 3166-2.
- `CloudFront-Viewer-Country-Region-Name` – Contient le nom de la région de l'utilisateur. La région est la subdivision de premier niveau (la plus large ou la moins spécifique) du code ISO 3166-2.
- `CloudFront-Viewer-Latitude` – Contient la latitude approximative de l'utilisateur.
- `CloudFront-Viewer-Longitude` – Contient la longitude approximative de l'utilisateur.
- `CloudFront-Viewer-Metro-Code` – Contient le code régional de l'utilisateur. Ceci n'est présent que lorsque l'utilisateur est aux États-Unis.
- `CloudFront-Viewer-Postal-Code` – Contient le code postal de l'utilisateur.
- `CloudFront-Viewer-Time-Zone` Contient le fuseau horaire de l'utilisateur, au format de base de données de fuseau horaire IANA (par exemple, `America/Los_Angeles`).

> **Note**
>
> `CloudFront-Viewer-City`, `CloudFront-Viewer-Metro-Code` et `CloudFront-Viewer-Postal-Code` peuvent ne pas être disponibles pour chaque adresse IP. Certaines adresses IP ne peuvent pas être géolocalisées avec suffisamment de précision pour obtenir ces informations.

En-têtes permettant de déterminer la structure de l’en-tête de l’utilisateur

Vous pouvez ajouter les en-têtes suivants pour identifier l’utilisateur en fonction des en-têtes qu'il envoie. Par exemple, différents navigateurs peuvent envoyer des en-têtes HTTP dans un certain ordre. Si le navigateur spécifié dans l'en-tête `User-Agent` ne correspond pas à l'ordre d'en-tête attendu par ce navigateur, vous pouvez refuser la demande. De plus, si la valeur `CloudFront-Viewer-Header-Count` ne correspond pas au nombre d'en-têtes de `CloudFront-Viewer-Header-Order`, vous pouvez refuser la demande.

- `CloudFront-Viewer-Header-Order` : contient les noms d'en-tête de l'utilisateur dans l'ordre demandé, séparés par deux points. Par exemple : `CloudFront-Viewer-Header-Order: Host:User-Agent:Accept:Accept-Encoding`. Les en-têtes dépassant la limite de 7 680 caractères sont tronqués.
- `CloudFront-Viewer-Header-Count` : contient le nombre total d'en-têtes de l'utilisateur.

En-têtes liés à TLS

Vous pouvez ajouter les en-têtes suivants pour déterminer l' JA3 empreinte digitale, JA4 l'empreinte digitale et les détails de connexion TLS du spectateur :

- `CloudFront-Viewer-JA3-Fingerprint`— Contient l'JA3 empreinte digitale du spectateur. L' JA3 empreinte digitale peut vous aider à déterminer si la demande provient d'un client connu, s'il s'agit d'un logiciel malveillant ou d'un bot malveillant, ou d'une application attendue (liste autorisée).
- `CloudFront-Viewer-JA4-Fingerprint`— Contient l' JA4empreinte digitale du spectateur. Tout comme l' JA3 empreinte digitale, l'JA4 empreinte digitale peut vous aider à déterminer si la demande provient d'un client connu, s'il s'agit d'un logiciel malveillant ou d'un bot malveillant, ou d'une application attendue (liste autorisée). Vous pouvez utiliser l’empreinte pour constituer une base de données d’acteurs connus, fiables ou malveillants, à appliquer lors de l’inspection des demandes HTTP. Vous pouvez ensuite inspecter la valeur d'en-tête sur les serveurs Web de votre application ou dans vos Lambda @Edge et CloudFront Functions pour comparer la valeur d'en-tête à une liste d'empreintes de logiciels malveillants connus afin de bloquer les clients malveillants.
- `CloudFront-Viewer-TLS`— Contient la SSL/TLS version, le code et les informations relatives à la SSL/TLS poignée de main qui ont été utilisées pour établir la connexion entre le spectateur et. CloudFront Spécifiez la valeur au format suivant :

```
SSL/TLS_version:cipher:handshake_information
```

Pour *handshake_information*, l'en-tête peut contenir les valeurs suivantes :

- `fullHandshake`— Une poignée de main complète a été effectuée pendant la SSL/TLS session.
- `sessionResumed`— Une SSL/TLS session précédente a été reprise.
- `connectionReused`— Une SSL/TLS connexion précédente a été réutilisée.

Voici quelques exemples de valeurs pour cet en-tête.

```
TLSv1.3:TLS_AES_128_GCM_SHA256:sessionResumed
```

```
TLSv1.2:ECDHE-ECDSA-AES128-GCM-SHA256:connectionReused
```

```
TLSv1.1:ECDHE-RSA-AES128-SHA256:fullHandshake
```

```
TLSv1:ECDHE-RSA-AES256-SHA:fullHandshake
```

Pour la liste complète des SSL/TLS versions et des chiffrements possibles pouvant figurer dans cette valeur d'en-tête, consultez. the section called “Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront”

> **Remarques**
>
> - Les JA4 empreintes digitales JA3 et sont dérivées du SSL/TLS `Client Hello` paquet. Elles ne sont présentes que pour les demandes HTTPS.
> - Ces en-têtes liés à TLS peuvent être ajoutés à une politique de demande d’origine, mais ne peuvent pas être inclus dans une politique de cache.

Autres CloudFront en-têtes

Vous pouvez ajouter les en-têtes suivants pour déterminer l’URI de la demande initiale de l’utilisateur, les paramètres et valeurs de la chaîne de demande d’origine, ainsi que le protocole et la version :

- `CloudFront-Error-Uri` : contient l’URI de la demande d’origine reçue de l’utilisateur.

- `CloudFront-Error-Args` : contient les paramètres et les valeurs de la chaîne de demande d'origine.
- `CloudFront-Forwarded-Proto` – Contient le protocole de la demande de l'utilisateur (HTTP ou HTTPS).
- `CloudFront-Viewer-Http-Version` – Contient la version HTTP de la demande de l'utilisateur.

Comprendre comment les politiques de demande d'origine et les politiques de cache fonctionnent ensemble

Vous pouvez utiliser une politique de demande CloudFront d'origine pour contrôler les demandes CloudFront envoyées à l'origine, appelées demandes d'origine. Pour utiliser une politique de demande d'origine, vous devez attacher une politique de cache au même comportement de cache. Vous ne pouvez pas utiliser de stratégie de demande d'origine dans un comportement de cache sans stratégie de cache. Pour plus d'informations, consultez Contrôle des demandes d'origine à l'aide d'une stratégie.

Les politiques de demande d'origine et les politiques de cache fonctionnent ensemble pour déterminer les valeurs à CloudFront inclure dans les demandes d'origine. Toutes les chaînes de requête URL, tous les en-têtes HTTP et tous les cookies que vous spécifiez dans la clé de cache (à l'aide d'une politique de cache) sont automatiquement inclus dans les demandes d'origine. Toutes les chaînes de requête, tous les en-têtes et tous les cookies supplémentaires que vous spécifiez dans une politique de demande d'origine sont également inclus dans les demandes d'origine (mais pas dans la clé de cache).

Les politiques de demande d'origine et les politiques de cache comportent des paramètres qui peuvent sembler contradictoires. Par exemple, une politique peut autoriser certaines valeurs tandis qu'une autre les bloque. Le tableau suivant explique quelles valeurs sont CloudFront incluses dans les demandes d'origine lorsque vous utilisez conjointement les paramètres d'une politique de demande d'origine et d'une politique de cache. Ces paramètres s'appliquent généralement à tous les types de valeurs : chaînes de requête, en-têtes et cookies. Cependant, dans une politique de cache, vous ne pouvez pas spécifier tous les en-têtes ni utiliser une liste d'en-têtes bloquée.

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
Politique de cache				
Aucun	Aucune valeur provenant de la demande de visionnage n'est incluse dans la demande d'origine, à l'exception des valeurs par défaut incluses dans chaque demande d'origine. Pour plus d'informations, consultez Contrôle des demandes d'origine à l'aide d'une stratégie.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Seules les valeurs spécifiées dans la politique de demande d'origine sont incluses dans la demande d'origine.	Toutes les valeurs de la demande de visionnage à l'exception de celles spécifiées dans la politique de demande d'origine sont incluses dans la demande d'origine.
Tous Remarque : Vous ne pouvez pas spécifier tous les en-têtes dans une politique de cache.	Toutes les chaînes de requête et tous les cookies de la demande de visionnage sont inclus dans la demande d'origine.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Toutes les chaînes de requête et tous les cookies de la demande de visionnage, ainsi que tous les en-têtes spécifiés dans la politique de demande	Toutes les chaînes de requête et tous les cookies de la demande de visionnage sont inclus dans la demande d'origine, même ceux spécifiés

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
			d'origine sont inclus dans la demande d'origine.	dans la liste de blocages de la politique de demande d'origine. Le paramètre de politique de cache remplace la liste de blocages de la politique de demande d'origine.

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
Liste verte	Seules les valeurs spécifiées dans la demande de visionnage sont incluses dans la demande d'origine.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Toutes les valeurs spécifiées dans la politique de cache ou dans la politique de demande d'origine sont incluses dans la demande d'origine.	Les valeurs spécifiées dans la politique de cache sont incluses dans la demande d'origine, même si ces mêmes valeurs sont spécifiées dans la liste de blocages de la politique de demande d'origine. La liste verte de la politique de cache remplace la liste de blocages de la politique de demande d'origine.

	Politique de demande d'origine			
	Aucun	Tous	Liste verte	Liste de blocages
Liste de blocages Remarque : Vous ne pouvez pas spécifier d'en-têtes dans la liste de blocages d'une politique de cache.	Toutes les chaînes de requête et tous les cookies de la demande de visionnage à l'exception de ceux spécifiés sont inclus dans la demande d'origine.	Toutes les valeurs de la demande de visionnage sont incluses dans la demande d'origine.	Les valeurs spécifiées dans la politique de demande d'origine sont incluses dans la demande d'origine, même si ces mêmes valeurs sont spécifiées dans la liste de blocages de la politique de cache. La liste verte de la politique de demande d'origine remplace la liste de blocages de la politique de cache.	Toutes les valeurs de la demande de visionnage à l'exception de celles spécifiées dans la politique de cache ou dans la politique de demande d'origine sont incluses dans la demande d'origine.

Ajouter ou supprimer des en-têtes HTTP dans les CloudFront réponses avec une politique

Vous pouvez configurer CloudFront pour modifier les en-têtes HTTP dans les réponses qu'il envoie aux spectateurs (navigateurs Web et autres clients). CloudFront peut supprimer les en-têtes qu'il a reçus de l'origine, ou ajouter des en-têtes à la réponse, avant de l'envoyer aux spectateurs. Ces modifications ne nécessitent pas d'écrire de code ou de modifier l'origine.

Par exemple, vous pouvez supprimer des en-têtes tels que `X-Powered-By` et `Vary` afin de CloudFront ne pas les inclure dans les réponses qu'il envoie aux spectateurs. Vous pouvez également ajouter des en-têtes HTTP tels que les suivants :

- Un en-tête `Cache-Control` pour contrôler la mise en cache du navigateur.
- Un en-tête `Access-Control-Allow-Origin` pour activer le partage des ressources cross-origin (Cross-Origin Resource Sharing, CORS). Vous pouvez également ajouter d'autres en-têtes CORS.
- Un ensemble d'en-têtes de sécurité courants, tels que `Strict-Transport-Security`, `Content-Security-Policy` et `X-Frame-Options`.
- Un `Server-Timing` en-tête pour afficher les informations relatives aux performances et au routage de la demande et de la réponse CloudFront.

Pour spécifier les en-têtes à CloudFront ajouter ou à supprimer dans les réponses HTTP, vous utilisez une politique d'en-têtes de réponse. Vous associez une politique d'en-têtes de réponse à un ou plusieurs comportements de cache. CloudFront modifie les en-têtes des réponses qu'il envoie aux requêtes qui correspondent au comportement du cache. CloudFrontmodifie les en-têtes des réponses qu'il diffuse depuis le cache et celles qu'il transmet depuis l'origine. Si la réponse d'origine inclut un ou plusieurs en-têtes ajoutés dans une politique d'en-têtes de réponse, la stratégie peut spécifier si elle CloudFront utilise l'en-tête qu'elle a reçu de l'origine ou si elle remplace cet en-tête par celui de la politique d'en-têtes de réponse.

> **Note**
>
> Si vous ajoutez des en-têtes qui contrôlent la mise en cache du navigateur à vos politiques d'en-tête de réponse, par exemple, si vous ajoutez ces CloudFront en-têtes à la réponse de l'utilisateur uniquement. *`Cache-Control`* Ces en-têtes n'ont aucune incidence sur la façon dont l'objet demandé est CloudFront mis en cache.

CloudFront fournit des politiques d'en-têtes de réponse prédéfinies, appelées politiques gérées, pour les cas d'utilisation courants. Vous pouvez utiliser ces politiques gérées ou créer vos propres politiques. Vous pouvez associer une politique d'en-têtes de réponse unique à plusieurs comportements de cache dans plusieurs distributions de votre Compte AWS.

Pour plus d’informations, consultez les ressources suivantes :

Rubriques

- Comprendre les politiques d’en-têtes de réponses
- Création de politiques d’en-têtes de réponses
- Utilisation de politiques d’en-têtes de réponse gérées

Comprendre les politiques d’en-têtes de réponses

Vous pouvez utiliser une politique d'en-têtes de réponse pour spécifier les en-têtes HTTP qu'Amazon CloudFront supprime ou ajoute dans les réponses qu'il envoie aux spectateurs. Pour plus d’informations sur les politiques d’en-têtes de réponses et sur les raisons de leur utilisation, consultez la section Ajout ou suppression d’en-têtes de réponse à l’aide d’une politique.

Les rubriques suivantes expliquent les paramètres dans une politique d’en-têtes de réponses. Les paramètres sont regroupés en catégories, qui sont représentées dans les rubriques suivantes.

Rubriques

- Détails de la politique (métadonnées)
- En-têtes CORS
- En-têtes de sécurité
- En-têtes personnalisés
- Suppression d’en-têtes
- Server-Timing en-tête

Détails de la politique (métadonnées)

Les paramètres des détails de la politique contiennent des métadonnées sur une politique d'en-têtes de réponses.

- Name (Nom) : nom permettant d'identifier la politique d’en-têtes de réponses. Dans la console, utilisez le nom pour attacher la politique à un comportement de cache.
- Description (facultative) : commentaire permettant de décrire la politique d’en-têtes de réponses. Cette option est facultative, mais elle peut vous aider à identifier l'objectif de la politique.

En-têtes CORS

Les paramètres de partage des ressources cross-origin (CORS) permettent d'ajouter et de configurer des en-têtes CORS dans une politique d'en-têtes de réponses.

Cette liste explique comment spécifier des paramètres et des valeurs valides dans une politique d’en-têtes de réponse. Pour plus d'informations sur chacun de ces en-têtes et sur leur mode d’utilisation pour les demandes et réponses CORS réelles, consultez la section partage des ressources cross-origin dans MDN Web Docs et dans les spécifications de protocole CORS.

Access-Control-Allow-Credentials

Il s'agit d'un paramètre booléen (`true`ou`false`) qui détermine si l'`Access-Control-Allow-Credentials`en-tête est CloudFront ajouté aux réponses aux requêtes CORS. Lorsque ce paramètre est défini sur`true`, CloudFront ajoute l'`Access-Control-Allow-Credentials: true`en-tête dans les réponses aux requêtes CORS. Sinon, CloudFront n'ajoute pas cet en-tête aux réponses.

Access-Control-Allow-Headers

Spécifie les noms d'en-tête qui sont CloudFront utilisés comme valeurs pour l'`Access-Control-Allow-Headers`en-tête dans les réponses aux demandes de précontrôle CORS. Les valeurs valides pour ce paramètre incluent les noms d'en-têtes HTTP ou le caractère générique (`*`), qui indique que tous les en-têtes sont admis.

> **Note**
>
> L’en-tête `Authorization` ne peut pas utiliser de caractère générique et doit être répertorié explicitement.

Exemples d'utilisation valide du caractère générique

Exemple	Correspond à	Ne correspond pas à
`x-amz-*`	`x-amz-test` `x-amz-`	`x-amz`
`x-*-amz`	`x-test-amz` `x--amz`	
`*`	Tous les en-têtes sauf `Authorization`	`Authorization`

Access-Control-Allow-Methods

Spécifie les méthodes HTTP qui sont CloudFront utilisées comme valeurs pour l'`Access-Control-Allow-Methods`en-tête dans les réponses aux requêtes CORS Preflight. Les valeurs valides sont `GET`, `DELETE`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT` et `ALL`. `ALL` est une valeur spéciale qui inclut toutes les méthodes HTTP répertoriées.

Access-Control-Allow-Origin

Spécifie les valeurs qui CloudFront peuvent être utilisées dans l'en-tête de `Access-Control-Allow-Origin` réponse. Les valeurs valides pour ce paramètre incluent une origine spécifique (telle que `http://www.example.com`) ou le caractère générique (`*`), ce qui indique que toutes les origines sont autorisées.

> **Remarques**
>
> - Le caractère générique (`*`) est autorisé à l'extrémité gauche du sous-domaine (`*.example.org`).
> - Le caractère générique (`*`) n'est pas autorisé aux positions suivantes :
>   - Top-level domaines (`example.*`)
>   - À droite des sous-domaines (`test.*.example.org`) ou au sein de n'importe quel sous-domaine (`*test.example.org`)
>   - À l'intérieur des termes (`exa*mple.org`)

Pour obtenir des exemples d'utilisation du caractère générique, consultez le tableau suivant.

Exemple	Correspond à	Ne correspond pas à

`http://*.example.org`	`http://www.example.org`
	
	`http://test.example.org`
		`https``://test.example.org`
		
		`https``://test.example.org:123`
		
		`http://test.example.org:123`

`*.example.org`	`test.example.org`
	
	`test.test.example.org`
	
	`.example.org`
	
	`http://test.example.org`
	
	`https://test.example.org`
		`http://test.example.org:123`
		
		`https://test.example.org:123`

`example.org`	`http://example.org`
	
	`https://example.org`	

`http://example.org`		**`https`**`://example.org` `http://example.org:123`

`http://example.org:*`	`http://example.org:123`
	
	`http://example.org`	

Exemple	Correspond à	Ne correspond pas à

`http://example.org:1*3`	`http://example.org:123`
	
	`http://example.org:1893`
	
	`http://example.org:13`	

`*.example.org:1*`	`test.example.org:123`	

Access-Control-Expose-Headers

Spécifie les noms d'en-tête qui sont CloudFront utilisés comme valeurs pour l'`Access-Control-Expose-Headers`en-tête dans les réponses aux requêtes CORS. Les valeurs valides pour ce paramètre incluent les noms d'en-têtes HTTP ou le caractère générique (`*`).

Access-Control-Max-Age

Nombre de secondes, qui est CloudFront utilisé comme valeur pour l'`Access-Control-Max-Age`en-tête dans les réponses aux demandes de pré-contrôle CORS.

Origin override (Remplacement de l’origine)

Paramètre booléen qui détermine le CloudFront comportement lorsque la réponse provenant de l'origine contient l'un des en-têtes CORS qui figurent également dans la politique.

- Lorsque ce paramètre est défini sur `true` et que la réponse d'origine contient un en-tête CORS qui figure également dans la politique, CloudFront ajoute l'en-tête CORS de la politique à la réponse. CloudFront envoie ensuite cette réponse au spectateur. CloudFront ignore l'en-tête qu'il a reçu de l'origine.
- Lorsqu'il est défini sur `false` et que la réponse d'origine contient un en-tête CORS (que l'en-tête CORS figure ou non dans la politique), CloudFront inclut l'en-tête CORS qu'elle a reçu de l'origine dans la réponse. CloudFront n'ajoute aucun en-tête CORS dans la politique à la réponse envoyée au spectateur.

En-têtes de sécurité

Vous pouvez utiliser les paramètres des en-têtes de sécurité pour ajouter et configurer plusieurs en-têtes de réponse HTTP liés à la sécurité dans une politique d'en-têtes de réponse.

Cette liste explique comment vous pouvez spécifier le paramètre et les valeurs valides dans une politique d'en-têtes de réponse. Pour plus d'informations sur chacun de ces en-têtes et sur leur mode d'utilisation dans les réponses HTTP réelles, consultez les liens d'accès à MDN Web Docs.

Content-Security-Policy

Spécifie les directives de politique de sécurité du contenu qui sont CloudFront utilisées comme valeurs pour l'en-tête de `Content-Security-Policy` réponse.

Pour plus d'informations sur cet en-tête et sur les directives valides de la politique, consultez la section Content-Security-Policy dans MDN Web Docs.

> **Note**
>
> La valeur d'en-tête `Content-Security-Policy` est limitée à 1 783 caractères.

Referrer-Policy

Spécifie la directive de politique de référent qui est CloudFront utilisée comme valeur pour l'en-tête de `Referrer-Policy` réponse. Les valeurs valides pour ce paramètre sont `no-referrer`, `no-referrer-when-downgrade`, `origin`, `origin-when-cross-origin`, `same-origin`, `strict-origin`, `strict-origin-when-cross-origin` et `unsafe-url`.

Pour plus d'informations sur cet en-tête et ces directives, consultez la section Referrer-Policy dans MDN web Docs.

Strict-Transport-Security

Spécifie les directives et les paramètres CloudFront utilisés comme valeur pour l'en-tête de `Strict-Transport-Security` réponse. Pour ce paramètre, spécifiez séparément :

- Un nombre de secondes, qui est CloudFront utilisé comme valeur pour la `max-age` directive de cet en-tête
- Un paramètre booléen (`true`ou`false`) pour`preload`, qui détermine si la `preload` directive est CloudFront incluse dans la valeur de cet en-tête

- Un paramètre booléen (`true`ou`false`) pour`includeSubDomains`, qui détermine si la `includeSubDomains` directive est CloudFront incluse dans la valeur de cet en-tête

Pour plus d'informations sur cet en-tête et ces directives, consultez la section Strict-Transport-Security dans MDN web Docs.

X-Content-Type-Options

Il s'agit d'un paramètre booléen (`true`ou`false`) qui détermine si l'`X-Content-Type-Options`en-tête est CloudFront ajouté aux réponses. Lorsque ce paramètre est défini`true`, CloudFront ajoute l'`X-Content-Type-Options: nosniff`en-tête aux réponses. Sinon, cet en-tête CloudFront n'est pas ajouté.

Pour plus d'informations sur cet en-tête, consultez la section X-Content-Type-Options dans MDN Web Docs.

X-Frame-Options

Spécifie la directive CloudFront à utiliser comme valeur pour l'en-tête de `X-Frame-Options` réponse. Les valeurs valides pour ce paramètre sont `DENY` ou `SAMEORIGIN`.

Pour plus d'informations sur cet en-tête et ces directives, consultez la section X-Frame-Options dans MDN web Docs.

X-XSS-Protection

Spécifie les directives et les paramètres CloudFront utilisés comme valeur pour l'en-tête de `X-XSS-Protection` réponse. Pour ce paramètre, spécifiez séparément :

- Un paramètre `X-XSS-Protection` de `0` (désactive le filtrage XSS) ou `1` (active le filtrage XSS)
- Un paramètre booléen (`true`ou`false`) pour`block`, qui détermine si la `mode=block` directive est CloudFront incluse dans la valeur de cet en-tête
- Un URI de rapport, qui détermine si CloudFront la `report=`*`reporting URI`* directive est incluse dans la valeur de cet en-tête

Vous pouvez spécifier `true` pour `block`, ou une URI de génération de rapports, mais pas les deux conjointement. Pour plus d'informations sur cet en-tête et ces directives, consultez la section X-XSS-Protection dans MDN web Docs.

Origin override (Remplacement de l'origine)

Chacun de ces paramètres d'en-têtes de sécurité contient un paramètre booléen (`true`ou`false`) qui détermine le CloudFront comportement lorsque la réponse de l'origine contient cet en-tête.

Lorsque ce paramètre est défini sur `true` et que la réponse d'origine contient l'en-tête, CloudFront ajoute l'en-tête de la politique à la réponse qu'elle envoie au spectateur. Il ignore l'en-tête qu'il a reçu de l'origine.

Lorsque ce paramètre est défini sur `false` et que la réponse d'origine contient l'en-tête, CloudFront inclut l'en-tête qu'elle a reçu de l'origine dans la réponse qu'elle envoie au spectateur.

Lorsque la réponse d'origine ne contient pas d'en-tête, CloudFront ajoute l'en-tête de la politique à la réponse qu'elle envoie au spectateur. CloudFront effectue cette opération lorsque ce paramètre est réglé sur `true` ou`false`.

En-têtes personnalisés

Vous pouvez utiliser les paramètres d'en-têtes personnalisés pour ajouter et configurer des en-têtes HTTP personnalisés dans une politique d'en-têtes de réponse. CloudFront ajoute ces en-têtes à chaque réponse qu'il renvoie aux spectateurs. Pour chaque en-tête personnalisé, spécifiez également la valeur de l'en-tête, bien que la spécification d'une valeur soit facultative. Cela est dû au fait que CloudFront vous pouvez ajouter un en-tête de réponse sans valeur.

Chaque en-tête personnalisé possède également son propre paramètre Origin override (Remplacement de l’origine) :

- Lorsque ce paramètre est défini sur `true` et que la réponse d'origine contient l'en-tête personnalisé qui figure dans la politique, CloudFront ajoute l'en-tête personnalisé de la politique à la réponse qu'elle envoie au spectateur. Il ignore l'en-tête qu'il a reçu de l'origine.
- Lorsque ce paramètre est défini `false` et que la réponse d'origine contient l'en-tête personnalisé figurant dans la politique, CloudFront inclut l'en-tête personnalisé qu'elle a reçu de l'origine dans la réponse qu'elle envoie au spectateur.
- Lorsque la réponse d'origine ne contient pas l'en-tête personnalisé qui figure dans la politique, CloudFront ajoute l'en-tête personnalisé de la politique à la réponse qu'elle envoie au spectateur. CloudFront effectue cette opération lorsque ce paramètre est réglé sur `true` ou`false`.

Suppression d’en-têtes

Vous pouvez spécifier les en-têtes que vous CloudFront souhaitez supprimer des réponses qu'il reçoit de l'origine afin qu'ils ne soient pas inclus dans les réponses CloudFront envoyées aux spectateurs. CloudFront supprime les en-têtes de chaque réponse qu'il envoie aux spectateurs, que

les objets soient servis depuis le CloudFront cache ou depuis l'origine. Par exemple, vous pouvez supprimer les en-têtes qui ne sont d'aucune utilité pour les navigateurs, tels que `X-Powered-By` ou`Vary`, afin de CloudFront supprimer ces en-têtes des réponses qu'il envoie aux spectateurs.

Lorsque vous spécifiez des en-têtes à supprimer à l'aide d'une politique d'en-têtes de réponse, CloudFront supprimez d'abord les en-têtes, puis ajoutez tous les en-têtes spécifiés dans d'autres sections de la politique d'en-têtes de réponse (en-têtes CORS, en-têtes de sécurité, en-têtes personnalisés, etc.). Si vous spécifiez un en-tête à supprimer mais que vous ajoutez également le même en-tête dans une autre section de la politique, CloudFront incluez l'en-tête dans les réponses qu'il envoie aux spectateurs.

> **Note**
>
> Vous pouvez utiliser une politique d'en-têtes de réponse pour supprimer les `Date` en-têtes `Server` et qui CloudFront ont été reçus de l'origine, afin que ces en-têtes (tels qu'ils ont été reçus de l'origine) ne soient pas inclus dans les réponses CloudFront envoyées aux spectateurs. Toutefois, si vous le faites, il CloudFront ajoute sa propre version de ces en-têtes aux réponses qu'il envoie aux spectateurs. Pour l'`Server`en-tête qui CloudFront ajoute, la valeur de l'en-tête est`CloudFront`.

En-têtes que vous ne pouvez pas supprimer

Vous ne pouvez pas supprimer les en-têtes suivants à l'aide d'une politique d'en-têtes de réponse. Si vous spécifiez ces en-têtes dans la section Remove headers (Supprimer les en-têtes) d'une politique d'en-têtes de réponse (`ResponseHeadersPolicyRemoveHeadersConfig` dans l'API), vous recevez un message d'erreur.

- `Connection`
- `Content-Encoding`
- `Content-Length`
- `Expect`
- `Host`
- `Keep-Alive`
- `Proxy-Authenticate`
- `Proxy-Authorization`

- Proxy-Connection
- Trailer
- Transfer-Encoding
- Upgrade
- Via
- Warning
- X-Accel-Buffering
- X-Accel-Charset
- X-Accel-Limit-Rate
- X-Accel-Redirect
- X-Amz-Cf-.*
- X-Amzn-Auth
- X-Amzn-Cf-Billing
- X-Amzn-Cf-Id
- X-Amzn-Cf-Xff
- X-Amzn-ErrorType
- X-Amzn-Fle-Profile
- X-Amzn-Header-Count
- X-Amzn-Header-Order
- X-Amzn-Lambda-Integration-Tag
- X-Amzn-RequestId
- X-Edge-.*
- X-Forwarded-Proto
- X-Real-Ip

Server-Timing en-tête

Utilisez le paramètre Server-Timing d'en-tête pour activer l'Server-Timingen-tête dans les réponses HTTP envoyées depuis CloudFront. Vous pouvez utiliser cet en-tête pour afficher

des statistiques qui peuvent vous aider à mieux comprendre le comportement, les performances CloudFront et votre origine. Par exemple, vous pouvez voir quelle couche de cache a généré un accès au cache. Vous pouvez également voir la latence du premier octet à partir de l'origine en cas d'échec d'accès au cache Les mesures figurant dans l'`Server-Timing`en-tête peuvent vous aider à résoudre les problèmes ou à tester l'efficacité de votre configuration CloudFront ou de celle d'origine.

Pour plus d'informations sur l'utilisation de l'`Server-Timing`en-tête avec CloudFront, consultez les rubriques suivantes.

Pour activer l'en-tête `Server-Timing`, créez (ou modifiez) une politique d'en-têtes de réponse.

Rubriques

- Taux d'échantillonnage et en-tête de requête Pragma
- Server-Timing en-tête depuis l'origine
- Server-Timing métriques d'en-tête
- Server-Timing exemples d'en-têtes

Taux d'échantillonnage et en-tête de requête Pragma

Lorsque vous activez l'en-tête `Server-Timing` dans une politique d'en-têtes de réponse, spécifiez également le taux d'échantillonnage. La fréquence d'échantillonnage est un nombre compris entre 0 et 100 (inclus) qui indique le pourcentage de réponses auxquelles vous CloudFront souhaitez ajouter l'`Server-Timing`en-tête. Lorsque vous définissez la fréquence d'échantillonnage sur 100, CloudFront ajoute l'`Server-Timing`en-tête à la réponse HTTP pour chaque demande qui correspond au comportement du cache auquel la politique d'en-têtes de réponse est attachée. Lorsque vous le définissez sur 50, CloudFront ajoute l'en-tête à 50 % des réponses pour les demandes qui correspondent au comportement du cache. Vous pouvez définir le taux d'échantillonnage sur n'importe quelle valeur comprise entre 0 et 100, avec quatre décimales au maximum.

Lorsque la fréquence d'échantillonnage est définie sur un nombre inférieur à 100, vous ne pouvez pas contrôler les réponses auxquelles l'`Server-Timing`en-tête est CloudFront ajouté, mais uniquement le pourcentage. Toutefois, vous pouvez ajouter l'en-tête `Pragma` avec une valeur définie sur `server-timing` dans une demande HTTP pour recevoir l'en-tête `Server-Timing` dans la réponse à cette demande. Cela fonctionne quel que soit le taux d'échantillonnage défini. Même lorsque la fréquence d'échantillonnage est réglée sur zéro (0), CloudFront ajoute l'`Server-Timing`en-tête à la réponse si la demande contient cet `Pragma: server-timing` en-tête.

Server-Timing en-tête depuis l'origine

Lorsqu'une erreur de cache survient et CloudFront que la demande est transmise à l'origine, celle-ci peut inclure un `Server-Timing` en-tête dans sa réponse à CloudFront. Dans ce cas, CloudFront ajoute ses métriques à l'`Server-Timing`en-tête qu'il a reçu de l'origine. La réponse envoyée CloudFront à l'utilisateur contient un seul `Server-Timing` en-tête qui inclut la valeur provenant de l'origine et les métriques CloudFront ajoutées. La valeur d'en-tête de l'origine peut se trouver à la fin ou entre deux ensembles de mesures qui s' CloudFront ajoutent à l'en-tête.

En cas d'accès au cache, la réponse envoyée au CloudFront visualiseur contient un seul `Server-Timing` en-tête qui inclut uniquement les CloudFront métriques dans la valeur de l'en-tête (la valeur de l'origine n'est pas incluse).

Server-Timing métriques d'en-tête

Lorsque CloudFront vous ajoutez l'`Server-Timing`en-tête à une réponse HTTP, la valeur de l'en-tête contient une ou plusieurs mesures qui peuvent vous aider à obtenir des informations sur le comportement, les performances CloudFront et votre origine. La liste suivante contient toutes les métriques et leurs valeurs potentielles. Un `Server-Timing` en-tête ne contient que certaines de ces mesures, en fonction de la nature de la demande et de la réponse CloudFront.

Certaines de ces métriques sont incluses dans l'en-tête `Server-Timing` avec un nom uniquement (sans valeur). D'autres sont composées d'un nom et d'une valeur. Lorsqu'une métrique a une valeur, le nom et la valeur sont séparés par un point-virgule (`;`). Lorsque l'en-tête contient plusieurs métriques, celles-ci sont séparées par une virgule (`,`).

cdn-cache-hit

: CloudFront a fourni une réponse depuis le cache sans faire de demande à l'origine.

cdn-cache-refresh

: CloudFront a fourni une réponse depuis le cache après avoir envoyé une demande à l'origine pour vérifier que l'objet mis en cache est toujours valide. Dans ce cas, CloudFront je n'ai pas récupéré l'objet complet depuis l'origine.

cdn-cache-miss

: CloudFront n'a pas fourni de réponse depuis le cache. Dans ce cas, CloudFront a demandé l'objet complet à l'origine avant de renvoyer la réponse.

cdn-pop

Contient une valeur qui décrit le CloudFront point de présence (POP) qui a traité la demande.

cdn-rid

Contient une valeur contenant l'identifiant CloudFront unique de la demande. Vous pouvez utiliser cet identifiant de demande (RID) lors du dépannage de problèmes liés à Support.

cdn-hit-layer

Cette métrique est présente lorsqu'elle CloudFront fournit une réponse depuis le cache sans adresser de requête à l'origine. Contient l'une des valeurs suivantes :

- EDGE : CloudFront a fourni la réponse mise en cache depuis un emplacement POP.
- REC : CloudFront a fourni la réponse mise en cache à partir d'un emplacement du cache périphérique régional (REC).
- Origin Shield : CloudFront a fourni la réponse mise en cache du REC qui fait office d'Origin Shield.

cdn-upstream-layer

Lorsque l'objet complet est CloudFront demandé à l'origine, cette métrique est présente et contient l'une des valeurs suivantes :

- EDGE : un emplacement POP a envoyé la demande directement à l'origine.
- REC : un emplacement REC a envoyé la demande directement à l'origine.
- Origin Shield : le REC qui agit en tant qu'Origin Shield a envoyé la demande directement à l'origine.

cdn-upstream-dns

Contient une valeur indiquant le nombre de millisecondes passées à récupérer l'enregistrement DNS pour l'origine. La valeur zéro (0) indique qu'un résultat DNS mis en cache a été CloudFront utilisé ou qu'une connexion existante a été réutilisée.

cdn-upstream-connect

Contient une valeur indiquant le nombre de millisecondes entre le moment où la demande DNS d'origine est terminée et une connexion TCP (et TLS, le cas échéant) à l'origine. La valeur zéro (0) indique qu'une connexion existante a CloudFront été réutilisée.

cdn-upstream-fbl

Contient une valeur indiquant le nombre de millisecondes entre le moment où la demande HTTP d'origine est terminée et le moment où le premier octet est reçu dans la réponse de l'origine (latence du premier octet).

cdn-downstream-fbl

Contient une valeur indiquant le nombre de millisecondes entre le moment où l'emplacement périphérique a fini de recevoir la demande et celui où il a envoyé le premier octet de la réponse à l'utilisateur.

Server-Timing exemples d'en-têtes

Voici des exemples d'`Server-Timing`en-tête qu'un utilisateur peut recevoir CloudFront lorsque le paramètre `Server-Timing` d'en-tête est activé.

Example– échec d'accès au cache

L'exemple suivant montre un `Server-Timing` en-tête qu'un utilisateur peut recevoir lorsque l'objet demandé n'est pas dans le CloudFront cache.

```
Server-Timing: cdn-upstream-layer;desc="EDGE",cdn-upstream-dns;dur=0,cdn-upstream-
connect;dur=114,cdn-upstream-fbl;dur=177,cdn-cache-miss,cdn-pop;desc="PHX50-C2",cdn-
rid;desc="yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==",cdn-downstream-
fbl;dur=436
```

Cet en-tête `Server-Timing` indique ce qui suit :

- La demande d'origine a été envoyée depuis un emplacement de CloudFront point de présence (POP) (`cdn-upstream-layer;desc="EDGE"`).
- CloudFront a utilisé un résultat DNS mis en cache pour l'origine (`cdn-upstream-dns;dur=0`).
- Il a fallu 114 millisecondes CloudFront pour terminer la connexion TCP (et TLS, le cas échéant) à l'origine (). `cdn-upstream-connect;dur=114`
- Il a fallu 177 millisecondes CloudFront pour recevoir le premier octet de la réponse de l'origine, après avoir terminé la requête (). `cdn-upstream-fbl;dur=177`
- L'objet demandé n'était pas dans CloudFront le cache (`cdn-cache-miss`).
- La demande a été reçue à l'emplacement périphérique identifié par le code `PHX50-C2`(`cdn-pop;desc="PHX50-C2"`).

- L'identifiant CloudFront unique de cette demande était `yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg==` (`cdn-rid;desc="yNPsyYn7skvTzwWkq3Wcc8Nj_foxUjQUe9H1ifslzWhb0w7aLbFvGg=="`).
- Il a fallu 436 millisecondes pour CloudFront envoyer le premier octet de la réponse au spectateur, après avoir reçu la requête du spectateur (). `cdn-downstream-fbl;dur=436`

Example– accès au cache

L'exemple suivant montre un `Server-Timing` en-tête qu'un utilisateur peut recevoir lorsque l'objet demandé est en CloudFront cache.

```
Server-Timing: cdn-cache-hit,cdn-pop;desc="SEA19-C1",cdn-
rid;desc="nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g==",cdn-hit-
layer;desc="REC",cdn-downstream-fbl;dur=137
```

Cet en-tête `Server-Timing` indique ce qui suit :

- L’objet demandé était dans le cache (`cdn-cache-hit`).
- La demande a été reçue à l’emplacement périphérique identifié par le code `SEA19-C1`(`cdn-pop;desc="SEA19-C1"`).
- L'identifiant CloudFront unique de cette demande était `nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g==` (`cdn-rid;desc="nQBz4aJU2kP9iC3KHEq7vFxfMozu-VYBwGzkW9diOpeVc7xsrLKj-g=="`).
- L’objet demandé a été mis en cache dans un emplacement REC (Regional Edge Cache) (`cdn-hit-layer;desc="REC"`).
- Il a fallu 137 millisecondes pour CloudFront envoyer le premier octet de la réponse au spectateur, après avoir reçu la requête du spectateur (). `cdn-downstream-fbl;dur=137`

Création de politiques d’en-têtes de réponses

Vous pouvez utiliser une politique d'en-têtes de réponse pour spécifier les en-têtes HTTP qu'Amazon CloudFront ajoute ou supprime dans les réponses HTTP. Pour plus d’informations sur les politiques d’en-têtes de réponses et sur les raisons de leur utilisation, consultez la section Ajout ou suppression d’en-têtes de réponse à l’aide d’une politique.

Vous pouvez créer une politique d'en-têtes de réponse dans la CloudFront console. Vous pouvez également en créer un AWS CloudFormation en utilisant le AWS Command Line Interface (AWS CLI)

ou l' CloudFront API. Après avoir créé une politique d'en-têtes de réponse, vous l'associez à un ou plusieurs comportements de cache dans une CloudFront distribution.

Avant de créer une politique d'en-têtes de réponse personnalisée, vérifiez si l'une des politiques d'en-têtes de réponse gérées est adaptée à votre cas d'utilisation. Si c'est le cas, vous pouvez l'attacher à votre comportement de cache. De cette façon, vous n'avez pas besoin de créer ou de gérer votre propre politique d'en-têtes de réponse.

Console

Pour créer une politique d'en-têtes de réponses (console)

1. Connectez-vous au Console de gestion AWS, puis accédez à l'onglet En-têtes de réponse sur la page Politiques de la CloudFront console à https://console.aws.amazon.com/cloudfront/v4/home#/policies/responseHeaders l'adresse.
2. Choisissez Create response headers policy (Créer une politique d'en-têtes de réponses).
3. Dans le formulaire Create response headers policy (Créer une politique d'en-têtes de réponses), procédez comme suit :

   a. Dans le panneau Details (Détails), saisissez un Name (Nom) pour la politique d'en-têtes de réponses et (éventuellement) une Description qui explique le rôle de la politique.

   b. Dans le panneau Cross-origin resource sharing (CORS) (Partage des ressources cross-origine [CORS]), choisissez le bouton bascule Configure CORS (Configurer CORS) et configurez tous les en-têtes CORS que vous souhaitez ajouter à la politique. Si vous souhaitez que les en-têtes configurés remplacent les en-têtes provenant de l'origine, cochez la case Remplacer l'origine. CloudFront

      Pour plus d'informations sur les paramètres d'en-têtes CORS, consultez la section the section called "En-têtes CORS".

   c. Dans Security headers (En-têtes de sécurité), choisissez le bouton bascule et configurez chacun des en-têtes de sécurité que vous souhaitez ajouter à la politique.

      Pour plus d'informations sur les paramètres des en-têtes de sécurité, consultez la section the section called "En-têtes de sécurité".

   d. Dans le panneau Custom headers (En-têtes personnalisés), ajoutez tous les en-têtes personnalisés que vous souhaitez inclure dans la politique.

Pour plus d'informations sur les paramètres d'en-têtes personnalisés, consultez la section the section called “En-têtes personnalisés”.

e. Dans le panneau Supprimer les en-têtes, ajoutez les noms des en-têtes que vous CloudFront souhaitez supprimer de la réponse de l'origine et ne pas inclure dans la réponse envoyée aux CloudFront spectateurs.

   Pour plus d'informations sur les paramètres de suppression d'en-têtes, consultez the section called “Suppression d’en-têtes”.

f. Dans le volet Server-Timing header (En-tête Server-Timing), sélectionnez l’option à bascule Enable (Activer) et saisissez un taux d'échantillonnage (nombre compris entre 0 et 100 inclus).

   Pour plus d'informations sur l'en-tête `Server-Timing`, consultez the section called “Server-Timing en-tête”.

4. Choisissez Create (Créer) pour créer la politique.

Après avoir créé une politique d'en-têtes de réponse, vous pouvez l'associer à un comportement de cache dans une CloudFront distribution.

Pour attacher une politique d’en-têtes de réponses à une distribution existante (console)

1. Ouvrez la page Distributions dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/distributions.
2. Choisissez la distribution à mettre à jour, puis choisissez l'onglet Behaviors (Comportements).
3. Sélectionnez le comportement du cache à mettre à jour, puis choisissez Edit (Modifier).

   Ou, pour créer un comportement de cache, choisissez Create behavior (Créer un comportement).
4. Pour Response headers policy (Politique d’en-têtes de réponses), choisissez la politique à ajouter au comportement du cache.
5. Choisissez Save changes (Enregistrer les modifications) pour mettre à jour le comportement du cache. [Si vous créez un comportement de cache, choisissez Create behavior (Créer un comportement)].

Pour attacher une politique d’en-têtes de réponses à une nouvelle distribution (console)

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create distribution (Créer une distribution).
3. Pour Response headers policy (Politique d’en-têtes de réponses), choisissez la politique à ajouter au comportement du cache.
4. Définissez les autres paramètres de votre distribution. Pour plus d’informations, consultez the section called “Tous les paramètres de distribution”.
5. Choisissez Create distribution (Créer une distribution) pour créer la distribution.

CloudFormation

Pour créer une politique d'en-têtes de réponse avec CloudFormation, utilisez le type de `AWS::CloudFront::ResponseHeadersPolicy` ressource. L'exemple suivant montre la syntaxe du CloudFormation modèle, au format YAML, pour créer une politique d'en-têtes de réponse.

```
Type: AWS::CloudFront::ResponseHeadersPolicy
Properties:
  ResponseHeadersPolicyConfig:
    Name: EXAMPLE-Response-Headers-Policy
    Comment: Example response headers policy for the documentation
    CorsConfig:
      AccessControlAllowCredentials: false
      AccessControlAllowHeaders:
        Items:
          - '*'
      AccessControlAllowMethods:
        Items:
          - GET
          - OPTIONS
      AccessControlAllowOrigins:
        Items:
          - https://example.com
          - https://docs.example.com
      AccessControlExposeHeaders:
        Items:
          - '*'
      AccessControlMaxAgeSec: 600
```

```
      OriginOverride: false
    CustomHeadersConfig:
      Items:
        - Header: Example-Custom-Header-1
          Value: value-1
          Override: true
        - Header: Example-Custom-Header-2
          Value: value-2
          Override: true
    SecurityHeadersConfig:
      ContentSecurityPolicy:
        ContentSecurityPolicy: default-src 'none'; img-src 'self'; script-src
 'self'; style-src 'self'; object-src 'none'; frame-ancestors 'none'
        Override: false
      ContentTypeOptions: # You don't need to specify a value for 'X-Content-Type-
Options'.
                          # Simply including it in the template sets its value to
 'nosniff'.
        Override: false
      FrameOptions:
        FrameOption: DENY
        Override: false
      ReferrerPolicy:
        ReferrerPolicy: same-origin
        Override: false
      StrictTransportSecurity:
        AccessControlMaxAgeSec: 63072000
        IncludeSubdomains: true
        Preload: true
        Override: false
      XSSProtection:
        ModeBlock: true # You can set ModeBlock to 'true' OR set a value for
 ReportUri, but not both
        Protection: true
        Override: false
    ServerTimingHeadersConfig:
      Enabled: true
      SamplingRate: 50
    RemoveHeadersConfig:
      Items:
        - Header: Vary
        - Header: X-Powered-By
```

Pour plus d'informations, consultez la section AWS::CloudFront::ResponseHeadersPolitique du guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer une politique d'en-têtes de réponse avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-response-headers-policy commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une politique d’en-têtes de réponses (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `response-headers-policy.yaml`. Ce fichier contient tous les paramètres d’entrée de la commande create-response-headers-policy.

```
aws cloudfront create-response-headers-policy --generate-cli-skeleton yaml-input
 > response-headers-policy.yaml
```

2. Ouvrez le fichier `response-headers-policy.yaml` que vous venez de créer. Modifiez le fichier pour spécifier un nom de politique et la configuration souhaitée pour la politique d'en-têtes de réponse, puis enregistrez le fichier.

   Pour plus d’informations sur les paramètres de la politique d’en-têtes de réponses, consultez la section the section called “Comprendre les politiques d’en-têtes de réponses”.

3. Utilisez la commande suivante pour créer une politique d'en-têtes de réponse. La politique que vous créez utilise les paramètres d'entrée du fichier `response-headers-policy.yaml`.

```
aws cloudfront create-response-headers-policy --cli-input-yaml file://response-
headers-policy.yaml
```

   Notez la valeur de `Id` dans la sortie de la commande. Il s'agit de l'ID de la politique d'en-têtes de réponse. Vous en avez besoin pour associer la politique au comportement du cache d'une CloudFront distribution.

Pour attacher une politique d'en-têtes de réponses à une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *distribution_ID* par l'ID de distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes au comportement de cache afin que celui-ci utilise la politique d'en-têtes de réponse.

   - Dans le comportement de cache, ajoutez un champ nommé `ResponseHeadersPolicyId`. Pour la valeur du champ, utilisez l'ID de politique d'en-têtes de réponse que vous avez noté après la création de la politique.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la politique d'en-têtes de réponses. Remplacez *distribution_ID* par l'ID de distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

Pour attacher une politique d'en-têtes de réponses à une nouvelle distribution (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `distribution.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-distribution.

```
aws cloudfront create-distribution --generate-cli-skeleton yaml-input >
 distribution.yaml
```

2. Ouvrez le fichier nommé `distribution.yaml` que vous venez de créer. Dans le comportement de cache par défaut, dans le champ `ResponseHeadersPolicyId`, saisissez l'ID de politique d'en-têtes de réponses que vous avez noté après la création de la politique. Poursuivez la modification du fichier pour spécifier les paramètres de distribution souhaité, puis enregistrez le fichier lorsque vous avez terminé.

   Pour plus d'informations sur les paramètres de distribution, consultez Référence de tous les paramètres de distribution.

3. Utilisez la commande suivante pour créer la distribution à l'aide des paramètres d'entrée du fichier `distribution.yaml`.

```
aws cloudfront create-distribution --cli-input-yaml file://distribution.yaml
```

API

Pour créer une politique d'en-têtes de réponse avec l' CloudFront API, utilisez CreateResponseHeadersPolicy. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez the section called "Comprendre les politiques d'en-têtes de réponses" la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une politique d'en-têtes de réponses, vous pouvez l'attacher à un comportement de cache, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de la politique d'en-têtes de demande dans le champ `ResponseHeadersPolicyId`, dans un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence de tous les paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Utilisation de politiques d’en-têtes de réponse gérées

Avec une politique d'en-têtes de CloudFront réponse, vous pouvez spécifier les en-têtes HTTP qu'Amazon CloudFront supprime ou ajoute dans les réponses qu'il envoie aux utilisateurs. Pour plus d’informations sur les politiques d’en-têtes de réponses et sur les raisons de leur utilisation, consultez la section Ajout ou suppression d’en-têtes de réponse à l’aide d’une politique.

CloudFront fournit des politiques d'en-têtes de réponse gérés que vous pouvez associer aux comportements du cache dans vos CloudFront distributions. Avec une politique d’en-têtes de réponses gérée, vous n'avez pas besoin d'écrire ou de gérer votre propre politique. Les politiques gérées contiennent des ensembles d'en-têtes de réponses HTTP pour les cas d'utilisation courants.

Pour utiliser une politique d’en-têtes de réponses gérée, attachez-la à un comportement de cache dans votre distribution. Le processus est le même que lorsque vous créez une politique d'en-têtes de réponse personnalisée. Toutefois, au lieu de créer une nouvelle politique, vous attachez l'une des politiques gérées. Vous joignez la politique soit par son nom (avec la console), soit par son identifiant (avec CloudFormation AWS CLI, le ou le AWS SDKs). Les noms et IDs les noms sont répertoriés dans la section suivante.

Pour de plus amples informations, veuillez consulter the section called “Création de politiques d’en-têtes de réponses”.

Les rubriques suivantes décrivent les politiques d'en-têtes de réponse gérées que vous pouvez utiliser.

Rubriques

- Cors-et- SecurityHeadersPolicy
- CORS-With-Preflight
- CORS- - with-preflight-and SecurityHeadersPolicy
- SecurityHeadersPolicy
- SimpleCORS

Cors-et- SecurityHeadersPolicy

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS simples de n'importe quelle origine. Cette politique ajoute également un ensemble d'en-têtes de sécurité à toutes les réponses

CloudFront envoyées aux spectateurs. Cette politique combine les politiques the section called “SimpleCORS” et the section called “SecurityHeadersPolicy” en une seule.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`e61eb60c-9c35-4d20-a928-2b84e02af89c`

Paramètres de politique

	Nom de l’en-tête	Valeur d’en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Origin`	`*`	Non
En-têtes de sécurité :	`Referrer-Policy`	`strict-origin-when-cross-origin`	Non
	`Strict-Transport-Security`	`max-age=31536000`	Non
	`X-Content-Type-Options`	`nosniff`	Oui
	`X-Frame-Options`	`SAMEORIGIN`	Non
	`X-XSS-Protection`	`1; mode=block`	Non

CORS-With-Preflight

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS de n'importe quelle origine, y compris les demandes de contrôle en amont. Pour les requêtes de pré-vol (à l'aide de la `OPTIONS` méthode HTTP), CloudFront ajoute les trois en-têtes suivants à la réponse. Pour les requêtes CORS simples, CloudFront ajoute uniquement l'`Access-Control-Allow-Origin`en-tête.

Si la réponse CloudFront reçue de l'origine inclut l'un de ces en-têtes, CloudFront utilise l'en-tête reçu (et sa valeur) dans sa réponse au spectateur. CloudFrontn'utilise pas l'en-tête dans cette politique.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`5cc3b908-e619-4b99-88e5-2cf7f45965bd`

Paramètres de politique

	Nom de l’en-tête	Valeur d’en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Methods`	`DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST`, `PUT`	Non
	`Access-Control-Allow-Origin`	`*`	
	`Access-Control-Expose-Headers`	`*`	

CORS- - with-preflight-and SecurityHeadersPolicy

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS de n'importe quelle origine. Cela inclut les demandes de contrôle en amont. Cette politique ajoute également un ensemble d'en-têtes de sécurité à toutes les réponses CloudFront envoyées aux spectateurs. Cette politique combine les politiques the section called “CORS-With-Preflight” et the section called “SecurityHeadersPolicy” en une seule.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`eaab4381-ed33-4a86-88ca-d9558dc6cd63`

Paramètres de politique

	Nom de l'en-tête	Valeur d'en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Methods`	`DELETE, GET, HEAD, OPTIONS, PATCH, POST, PUT`	Non
	`Access-Control-Allow-Origin`	`*`	
	`Access-Control-Expose-Headers`	`*`	
En-têtes de sécurité :	`Referrer-Policy`	`strict-origin-when-cross-origin`	Non
	`Strict-Transport-Security`	`max-age=31536000`	Non
	`X-Content-Type-Options`	`nosniff`	Oui
	`X-Frame-Options`	`SAMEORIGIN`	Non
	`X-XSS-Protection`	`1; mode=block`	Non

SecurityHeadersPolicy

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour ajouter un ensemble d'en-têtes de sécurité à toutes les réponses CloudFront envoyées aux utilisateurs. Pour plus d'informations sur ces en-têtes de sécurité, consultez les recommandations de sécurité web de Mozilla.

Avec cette politique d'en-têtes de réponse, des CloudFront ajouts `X-Content-Type-Options: nosniff` à toutes les réponses. C'est le cas lorsque la réponse CloudFront reçue de l'origine incluait cet en-tête et lorsque ce n'était pas le cas. Pour tous les autres en-têtes de cette politique, si la

réponse CloudFront reçue de l'origine inclut l'en-tête, CloudFront utilise l'en-tête reçu (et sa valeur) dans sa réponse au spectateur. Il n'utilise pas l'en-tête de cette politique.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`67f7725c-6f97-4210-82d7-5512b31e9d03`

Paramètres de politique

	Nom de l’en-tête	Valeur d’en-tête	Remplacer l'origine ?
En-têtes de sécurité :	`Referrer-Policy`	`strict-origin-when-cross-origin`	Non
	`Strict-Transport-Security`	`max-age=31536000`	Non
	`X-Content-Type-Options`	`nosniff`	Oui
	`X-Frame-Options`	`SAMEORIGIN`	Non
	`X-XSS-Protection`	`1; mode=block`	Non

SimpleCORS

Afficher cette politique dans la CloudFront console

Utilisez cette politique gérée pour autoriser les demandes CORS simples de n'importe quelle origine. Avec cette politique, CloudFront ajoute l'en-tête `Access-Control-Allow-Origin: *` à toutes les réponses pour les requêtes CORS simples.

Si la réponse CloudFront reçue de l'origine inclut l'`Access-Control-Allow-Origin`en-tête, CloudFront utilise cet en-tête (et sa valeur) dans sa réponse au spectateur. CloudFront n'utilise pas l'en-tête dans cette politique.

Lors de l'utilisation CloudFormation de l' AWS CLI API ou de l' CloudFront API, l'identifiant de cette politique est le suivant :

`60669652-455b-4ae9-85a4-c4c02393f86c`

Paramètres de politique

	Nom de l’en-tête	Valeur d’en-tête	Remplacer l'origine ?
En-têtes CORS :	`Access-Control-Allow-Origin`	*	Non

Comportement des demandes et des réponses

Les rubriques suivantes décrivent la façon dont CloudFront les demandes et les réponses sont traitées.

Vous pouvez découvrir comment CloudFront interagir avec Amazon S3 ou les origines personnalisées, gérer les différentes méthodes et en-têtes HTTP, traiter les codes d'état et gérer la mise en cache et les réponses aux erreurs.

Rubriques

- Comment CloudFront traiter les requêtes HTTP et HTTPS
- Comportement des demandes et des réponses pour les origines Amazon S3 Origins
- Comportement des demandes et des réponses pour les origines personnalisées
- Comportement des requêtes et des réponses pour les groupes d’origine
- Ajout d’en-têtes personnalisés aux demandes d’origine
- Comment CloudFront traite les demandes partielles pour un objet (range GETs)
- Comment CloudFront traite les codes d'état HTTP 3xx depuis votre origine
- Comment CloudFront traite les codes d'état HTTP 4xx et 5xx depuis votre origine
- Génération de réponses aux·erreurs personnalisées

Comment CloudFront traiter les requêtes HTTP et HTTPS

Pour les origines d'Amazon S3, CloudFront accepte par défaut les requêtes dans les protocoles HTTP et HTTPS pour les objets d'une CloudFront distribution. CloudFront transmet ensuite les demandes à votre compartiment Amazon S3 en utilisant le même protocole que celui dans lequel les demandes ont été effectuées.

Pour les origines personnalisées, lorsque vous créez une distribution, vous pouvez spécifier la manière dont CloudFront accède à votre origine : HTTP uniquement ou en adoptant le protocole utilisé par l'utilisateur. Pour plus d'informations sur la CloudFront gestion des requêtes HTTP et HTTPS pour des origines personnalisées, consultezProtocoles.

Pour plus d’informations sur la façon de restreindre votre distribution pour que les utilisateurs finaux puissent uniquement accéder aux objets à l’aide de HTTPS, consultez Utilisez le protocole HTTPS avec CloudFront.

> **Note**
>
> Les frais pour les requêtes HTTPS sont plus élevés que ceux pour les requêtes HTTP. Pour plus d'informations sur les taux de facturation, consultez la section CloudFront Tarification.

Comportement des demandes et des réponses pour les origines Amazon S3 Origins

Pour comprendre comment CloudFront traite les demandes et les réponses lorsque vous utilisez Amazon S3 comme origine, consultez les sections suivantes :

Rubriques

- Comment CloudFront traiter et transférer les demandes vers votre origine Amazon S3
- Comment CloudFront traite les réponses provenant de votre Amazon S3 origin

Comment CloudFront traiter et transférer les demandes vers votre origine Amazon S3

Découvrez comment CloudFront traite les demandes des spectateurs et les transmet à votre origine Amazon S3.

Table des matières

- Durée de conservation dans le cache et durée de vie minimale
- Adresses IP client
- Demandes GET conditionnelles
- Cookies
- Cross-origin partage de ressources (CORS)
- Demandes GET qui incluent un corps de texte
- Méthodes HTTP
- en-têtes de requête HTTP qui CloudFront suppriment ou mettent à jour
- Longueur maximale d’une demande et longueur maximale d’une URL
- OCSP Stapling

- Protocoles
- Chaînes de requête
- Délai d'attente et tentatives de connexion à l'origine
- Délai de réponse de l'origine
- Demandes simultanées pour le même objet (réduction des demandes)

Durée de conservation dans le cache et durée de vie minimale

Pour contrôler la durée pendant laquelle vos objets restent en CloudFront cache avant de CloudFront transmettre une autre demande à votre origine, vous pouvez :

- Configurer votre origine pour ajouter un `Cache-Control` ou un champ d'en-tête `Expires` à chaque objet.
- Spécifiez une valeur pour le TTL minimum dans les comportements CloudFront du cache.
- Utiliser la valeur par défaut de 24 heures.

Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Adresses IP client

Si un utilisateur envoie une demande à CloudFront et n'inclut pas d'en-tête de `X-Forwarded-For` demande, CloudFront il obtient son adresse IP à partir de la connexion TCP, ajoute un `X-Forwarded-For` en-tête qui inclut l'adresse IP et transmet la demande à l'origine. Par exemple, si CloudFront extrait l'adresse IP `192.0.2.2` de la connexion TCP, il transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.2
```

Si un utilisateur envoie une demande à CloudFront et inclut un en-tête de `X-Forwarded-For` demande, CloudFront obtient l'adresse IP du spectateur à partir de la connexion TCP, l'ajoute à la fin de l'`X-Forwarded-For`en-tête et transmet la demande à l'origine. Par exemple, si la demande du spectateur inclut `X-Forwarded-For: 192.0.2.4,192.0.2.3` et CloudFront obtient l'adresse IP `192.0.2.2` de la connexion TCP, elle transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

> **Note**
>
> L'en-tête `X-Forwarded-For` contient les adresses IPv4 (par exemple, 192.0.2.44) et les adresses IPv6 (par exemple, 2001:0db8:85a3::8a2e:0370:7334).
> Lorsque vous analysez des adresses IPv6 dans l'`X-Forwarded-For`en-tête, utilisez des bibliothèques d'analyse d'adresses IP standard capables de gérer n'importe quel format IPv6 RFC 4291 valide.

Demandes GET conditionnelles

Lorsqu'il CloudFront reçoit une demande concernant un objet qui a expiré depuis un cache périphérique, il transmet la demande à l'origine Amazon S3 pour obtenir la dernière version de l'objet ou pour obtenir la confirmation d'Amazon S3 que le cache CloudFront périphérique possède déjà la dernière version. Quand Amazon S3 a initialement envoyé l'objet à CloudFront, il a inclus une `ETag` valeur et une `LastModified` valeur dans la réponse. Dans la nouvelle demande qui est CloudFront transmise à Amazon S3, ajoutez CloudFront l'un des en-têtes suivants ou les deux :

- Un en-tête `If-Match` ou `If-None-Match` qui contient la valeur `ETag` pour la version expirée de l'objet.
- Un en-tête `If-Modified-Since` qui contient la valeur `LastModified` pour la version expirée de l'objet.

Amazon S3 utilise ces informations pour déterminer si l'objet a été mis à jour et, par conséquent, s'il faut renvoyer l'objet entier CloudFront ou uniquement un code d'état HTTP 304 (non modifié).

Cookies

Amazon S3 ne traite pas les cookies. Si vous configurez un comportement de cache pour transférer des cookies vers une origine Amazon S3, CloudFront vous transférez les cookies, mais Amazon S3 les ignore. Toutes les demandes futures pour le même objet, que vous faites varier le cookie ou non, sont servies à partir de l'objet existant dans le cache.

Cross-origin partage de ressources (CORS)

Si vous CloudFront souhaitez respecter les paramètres de partage des ressources entre origines d'Amazon S3, configurez CloudFront pour transférer les en-têtes sélectionnés vers Amazon S3. Pour plus d'informations, consultez Mise en cache de contenu basée sur des en-têtes de demandes.

Demandes GET qui incluent un corps de texte

Si une GET demande d'utilisateur inclut un corps, CloudFront renvoie un code d'état HTTP 403 (Interdit) au visualiseur.

Méthodes HTTP

Si vous configurez CloudFront pour traiter toutes les méthodes HTTP qu'il prend en charge, CloudFront accepte les demandes suivantes des spectateurs et les transmet à votre origine Amazon S3 :

- DELETE
- GET
- HEAD
- OPTIONS
- PATCH
- POST
- PUT

CloudFront met toujours en cache les réponses GET et les HEAD demandes. Vous pouvez également configurer CloudFront pour mettre en cache les réponses aux OPTIONS demandes. CloudFront ne met pas en cache les réponses aux demandes qui utilisent les autres méthodes.

Si vous souhaitez utiliser des chargements en plusieurs parties pour ajouter des objets à un compartiment Amazon S3, vous devez ajouter un contrôle CloudFront d'accès à l'origine (OAC) à votre distribution et accorder à l'OAC les autorisations nécessaires. Pour plus d'informations, consultez the section called “Restriction de l’accès à une origine Amazon S3”.

> **Important**
>
> Si vous configurez CloudFront pour accepter et transmettre à Amazon S3 toutes les méthodes HTTP prises CloudFront en charge, vous devez créer un CloudFront OAC pour restreindre l'accès à votre contenu Amazon S3 et accorder à l'OAC les autorisations requises. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes parce que vous souhaitez utiliser la PUT méthode, vous devez configurer les politiques de compartiment Amazon S3 pour gérer les DELETE demandes de manière appropriée afin que les utilisateurs ne puissent pas supprimer les ressources que vous ne souhaitez pas qu'ils

suppriment. Pour plus d'informations, consultez the section called "Restriction de l'accès à une origine Amazon S3".

Pour plus d'informations sur les opérations prises en charge par Amazon S3, consultez la documentation Amazon S3.

en-têtes de requête HTTP qui CloudFront suppriment ou mettent à jour

CloudFront supprime ou met à jour certains en-têtes avant de transmettre les demandes à votre origine Amazon S3. Pour la plupart des en-têtes, ce comportement est le même que pour les origines personnalisées. Pour obtenir la liste complète des en-têtes de requêtes HTTP et la manière dont ils CloudFront sont traités, consultezEn-têtes et CloudFront comportement des requêtes HTTP (origines personnalisées et Amazon S3).

Longueur maximale d'une demande et longueur maximale d'une URL

La longueur maximale d'une demande, y compris le chemin, la chaîne de requête (le cas échéant) et les en-têtes, est de 32 768 octets.

CloudFront construit une URL à partir de la demande. La longueur maximale de cette URL est de 8 192 caractères.

Si une URL dépasse la longueur maximale, CloudFront renvoie le code d'état HTTP 414 (URI trop long) à l'utilisateur. Si une demande dépasse la longueur maximale parce que la taille de l'en-tête est dépassée, CloudFront renvoie le code d'état HTTP 494 au visualiseur. Dans les deux cas, met CloudFront fin à la connexion TCP avec le visualiseur.

OCSP Stapling

Lorsqu'un utilisateur soumet une requête HTTPS pour un objet, CloudFront ou qu'il doit confirmer auprès de l'autorité de certification (CA) que le certificat SSL du domaine n'a pas été révoqué. L'agrafage OCSP accélère la validation des certificats en permettant de valider le certificat et de CloudFront mettre en cache la réponse de l'autorité de certification, de sorte que le client n'a pas besoin de valider le certificat directement auprès de l'autorité de certification.

L'amélioration des performances de l'agrafage OCSP est plus prononcée lors de la CloudFront réception de nombreuses requêtes HTTPS pour des objets du même domaine. Chaque serveur d'un emplacement périphérique CloudFront doit soumettre une demande de validation distincte. Lorsqu'il CloudFront reçoit un grand nombre de requêtes HTTPS pour le même domaine, chaque serveur

situé en périphérie reçoit rapidement une réponse de l'autorité de certification indiquant qu'il peut intégrer à un paquet lors de l'établissement de liaison SSL. Lorsque le spectateur est convaincu que le certificat est valide, il CloudFront peut servir l'objet demandé. Si votre distribution ne reçoit pas beaucoup de trafic dans un emplacement périphérique CloudFront , il est plus probable que les nouvelles demandes soient acheminées vers un serveur qui n'a pas encore validé le certificat auprès de l'autorité de certification. Dans ce cas, le visualiseur exécute séparément l'étape de validation et le CloudFront serveur sert l'objet. Ce CloudFront serveur soumet également une demande de validation à l'autorité de certification. Ainsi, la prochaine fois qu'il recevra une demande incluant le même nom de domaine, il recevra une réponse de validation de la part de l'autorité de certification.

Protocoles

CloudFront transmet les requêtes HTTP ou HTTPS au serveur d'origine en fonction du protocole de la demande du spectateur, HTTP ou HTTPS.

> **Important**
>
> Si votre compartiment Amazon S3 est configuré comme point de terminaison de site Web, vous ne pouvez pas le configurer CloudFront pour utiliser le protocole HTTPS pour communiquer avec votre point d'origine, car Amazon S3 ne prend pas en charge les connexions HTTPS dans cette configuration.

Chaînes de requête

Vous pouvez configurer si CloudFront les paramètres de chaîne de requête sont transférés à votre origine Amazon S3. Pour plus d'informations, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête.

Délai d'attente et tentatives de connexion à l'origine

Le délai d'expiration de la connexion à l'origine est le nombre de secondes qui CloudFront s'écoulent lors de la tentative d'établissement d'une connexion avec l'origine.

Les tentatives de connexion à l'origine sont le nombre de CloudFront tentatives de connexion à l'origine.

Ensemble, ces paramètres déterminent la durée pendant CloudFront laquelle vous essayez de vous connecter à l'origine avant de basculer vers l'origine secondaire (dans le cas d'un groupe d'origine)

ou de renvoyer une réponse d'erreur à l'utilisateur. Par défaut, CloudFront attend 30 secondes (3 tentatives de 10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d'attente de connexion plus court, ou les deux.

Pour plus d'informations, consultez Contrôle des délais d'expiration et des tentatives de l'origine.

Délai de réponse de l'origine

Le délai de réponse de l'origine, également appelé délai d'attente des opérations de lecture depuis l'origine ou délai de demande à l'origine, s'applique aux deux valeurs suivantes :

- Durée, en secondes, qui CloudFront attend une réponse après avoir transféré une demande à l'origine.
- Durée, en secondes, qui s'écoule CloudFront entre la réception d'un paquet d'une réponse de l'origine et la réception du paquet suivant.

CloudFront le comportement dépend de la méthode HTTP de la requête du visualiseur :

- `GET`et `HEAD` demandes : si l'origine ne répond pas dans les 30 secondes ou cesse de répondre pendant 30 secondes, CloudFront interrompt la connexion. Si le nombre spécifié de tentatives de connexion à l'origine est supérieur à 1, CloudFront essaie à nouveau d'obtenir une réponse complète. CloudFront essaie jusqu'à 3 fois, selon la valeur du paramètre Tentatives de connexion d'origine. Si l'origine ne répond pas lors de la dernière tentative, CloudFront ne réessaie pas tant qu'il ne reçoit pas une autre demande de contenu sur la même origine.
- `DELETE`,`OPTIONS`, `PATCH`PUT, et `POST` demandes : si l'origine ne répond pas dans les 30 secondes, CloudFront interrompt la connexion et n'essaie pas à nouveau de contacter l'origine. Le client peut soumettre à nouveau la demande si nécessaire.

Vous ne pouvez pas modifier le délai de réponse pour une origine Amazon S3 (un compartiment S3 qui n'est pas configuré avec un hébergement de site web statique).

Demandes simultanées pour le même objet (réduction des demandes)

Lorsqu'un emplacement CloudFront périphérique reçoit une demande pour un objet et que l'objet n'est pas dans le cache ou que l'objet mis en cache a expiré, envoie CloudFront immédiatement la demande à l'origine. Toutefois, s'il existe des demandes simultanées pour le même objet, c'est-à-dire si des demandes supplémentaires pour le même objet (avec la même clé de cache) arrivent

à l'emplacement périphérique avant de CloudFront recevoir la réponse à la première demande, CloudFront une pause s'arrête avant de transmettre les demandes supplémentaires à l'origine. Cette brève pause permet de réduire la charge sur l'origine. CloudFront envoie la réponse de la demande d'origine à toutes les demandes qu'il a reçues pendant sa pause. Ce processus se nomme la réduction des demandes. Dans CloudFront les journaux, la première demande est identifiée comme un `Miss` dans le `x-edge-result-type` champ, et les demandes réduites sont identifiées comme un`Hit`. Pour plus d'informations sur CloudFront les journaux, consultezthe section called "CloudFront et journalisation des fonctions Edge".

CloudFront réduit uniquement les requêtes qui partagent une clé de cache. Si les demandes supplémentaires ne partagent pas la même clé de cache parce que, par exemple, vous avez configuré CloudFront la mise en cache en fonction des en-têtes de demande, des cookies ou des chaînes de requête, CloudFront toutes les demandes avec une clé de cache unique sont transmises à votre origine.

Si vous souhaitez empêcher la fusion des demandes, vous pouvez utiliser la politique de cache gérée `CachingDisabled`, qui empêche également la mise en cache. Pour plus d'informations, consultez Utilisation des politiques de cache gérées.

Si vous souhaitez empêcher la fusion des demandes pour certains objets, vous pouvez définir la durée de vie minimale pour le comportement du cache sur 0 et configurer l'origine de sorte à envoyer `Cache-Control: private`, `Cache-Control: no-store`, `Cache-Control: no-cache`, `Cache-Control: max-age=0` ou `Cache-Control: s-maxage=0`. Ces configurations augmenteront la charge sur votre origine et introduiront une latence supplémentaire pour les demandes simultanées qui sont suspendues pendant l' CloudFront attente de la réponse à la première demande.

Comment CloudFront traite les réponses provenant de votre Amazon S3 origin

Découvrez comment CloudFront traite les réponses provenant de votre origine Amazon S3.

Table des matières

- Requêtes annulées
- en-têtes de réponse HTTP qui CloudFront suppriment ou mettent à jour
- Taille de fichier maximale pouvant être mise en cache
- Redirections

Requêtes annulées

Si un objet ne se trouve pas dans le cache périphérique et si un utilisateur met fin à une session (par exemple, ferme un navigateur) après avoir récupéré l'objet depuis votre origine mais avant de pouvoir livrer l'objet demandé, CloudFront ne CloudFront met pas l'objet en cache à l'emplacement périphérique.

en-têtes de réponse HTTP qui CloudFront suppriment ou mettent à jour

CloudFront supprime ou met à jour les champs d'en-tête suivants avant de transmettre la réponse depuis votre origine Amazon S3 au visualiseur :

- `X-Amz-Id-2`
- `X-Amz-Request-Id`
- `Set-Cookie`— Si vous configurez CloudFront pour transférer les cookies, le champ `Set-Cookie` d'en-tête sera transmis aux clients. Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.
- `Trailer`
- `Transfer-Encoding`— Si votre origine Amazon S3 renvoie ce champ d'en-tête, CloudFront définissez la valeur sur `chunked` avant de renvoyer la réponse à l'utilisateur.
- `Upgrade`
- `Via`— CloudFront définit la valeur suivante dans la réponse au spectateur :

  `Via: http-version alphanumeric-string.cloudfront.net (CloudFront)`

  Par exemple, la valeur ressemble à ce qui suit :

  `Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)`

Taille de fichier maximale pouvant être mise en cache

La taille maximale d'un corps de réponse enregistré CloudFront dans son cache est de 50 Go. Cette taille inclut les réponses de transfert fragmentées qui ne spécifient pas la valeur d'en-tête `Content-Length`.

Vous pouvez CloudFront utiliser la mise en cache d'un objet dont la taille est supérieure à cette taille en utilisant des requêtes de plage pour demander les objets par parties de 50 Go ou moins chacune. CloudFrontmet ces parties en cache car chacune d'elles fait 50 Go ou moins. Une fois que l'utilisateur

a récupéré toutes les parties de l'objet, il peut reconstruire l'objet d'origine plus large. Pour plus d'informations, consultez Utiliser les demandes de plage pour mettre en cache de large objets.

Redirections

Vous pouvez configurer un compartiment Amazon S3 pour rediriger toutes les demandes vers un autre nom d'hôte ; il peut s'agir d'un autre compartiment Amazon S3 ou d'un serveur HTTP. Si vous configurez un compartiment pour rediriger toutes les demandes et si le compartiment est à l'origine d'une CloudFront distribution, nous vous recommandons de configurer le compartiment pour rediriger toutes les demandes vers une CloudFront distribution en utilisant soit le nom de domaine de la distribution (par exemple, d111111abcdef8.cloudfront.net) soit un autre nom de domaine (un CNAME) associé à une distribution (par exemple, example.com). Dans le cas contraire, les requêtes du spectateur sont CloudFront contournées et les objets sont servis directement depuis la nouvelle origine.

> **Note**
>
> Si vous redirigez des demandes vers un nom de domaine alternatif, vous devez également mettre à jour le service DNS pour votre domaine en ajoutant un enregistrement CNAME. Pour plus d'informations, consultez Utilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME).

Voici ce qui se passe lorsque vous configurez un compartiment pour rediriger toutes les demandes :

1. Un visualiseur (par exemple, un navigateur) demande un objet à CloudFront.
2. CloudFront transmet la demande au compartiment Amazon S3 qui est à l'origine de votre distribution.
3. Amazon S3 renvoie un code de statut HTTP 301 (Déplacé de façon permanente), ainsi que le nouvel emplacement.
4. CloudFront met en cache le code d'état de redirection et le nouvel emplacement, et renvoie les valeurs à l'utilisateur. CloudFront ne suit pas la redirection pour récupérer l'objet depuis le nouvel emplacement.
5. Le visualiseur envoie une autre demande pour l'objet, mais cette fois, il spécifie le nouvel emplacement d'où il a été obtenu CloudFront :

    - Si le compartiment Amazon S3 redirige toutes les demandes vers une CloudFront distribution, en utilisant le nom de domaine de la distribution ou un autre nom de domaine, CloudFront

demande l'objet depuis le compartiment Amazon S3 ou le serveur HTTP du nouvel emplacement. Lorsque le nouvel emplacement renvoie l'objet, le CloudFront renvoie au visualiseur et le met en cache dans un emplacement périphérique.

- Si le compartiment Amazon S3 redirige les demandes vers un autre emplacement, la deuxième demande est ignorée CloudFront. Le compartiment Amazon S3 ou le serveur HTTP du nouvel emplacement renvoie l'objet directement au visualiseur, de sorte que l'objet n'est jamais mis en cache dans un cache CloudFront périphérique.

Comportement des demandes et des réponses pour les origines personnalisées

Pour comprendre comment CloudFront traite les demandes et les réponses lorsque vous utilisez des origines personnalisées, consultez les sections suivantes :

Rubriques

- Comment CloudFront traiter et transférer les demandes vers votre origine personnalisée
- Comment CloudFront traite les réponses provenant de votre origine personnalisée

Comment CloudFront traiter et transférer les demandes vers votre origine personnalisée

Découvrez comment CloudFront traite les demandes des spectateurs et les transmet à votre origine personnalisée.

Table des matières

- Authentification
- Durée de conservation dans le cache et durée de vie minimale
- Adresses IP client
- Client-side Authentification SSL
- Compression
- Demandes conditionnelles
- Cookies
- Cross-origin partage de ressources (CORS)

- Chiffrement
- Demandes GET qui incluent un corps de texte
- Méthodes HTTP
- En-têtes et CloudFront comportement des requêtes HTTP (origines personnalisées et Amazon S3)
- Version de HTTP
- Longueur maximale d'une demande et longueur maximale d'une URL
- OCSP Stapling
- Connexions persistantes
- Protocoles
- Chaînes de requête
- Délai d'attente et tentatives de connexion à l'origine
- Délai de réponse de l'origine
- Demandes simultanées pour le même objet (réduction des demandes)
- En-tête User-Agent

Authentification

Si vous transmettez l'en-tête `Authorization` à votre origine, vous pouvez ensuite configurer votre serveur d'origine pour demander une authentification du client pour les types de demandes suivants :

- `DELETE`
- `GET`
- `HEAD`
- `PATCH`
- `PUT`
- `POST`

Pour les `OPTIONS` demandes, l'authentification du client ne peut être configurée que si vous utilisez les CloudFront paramètres suivants :

- CloudFront est configuré pour transmettre l'`Authorization`en-tête à votre origine
- CloudFront est configuré pour ne pas mettre en cache la réponse aux `OPTIONS` demandes

Pour plus d'informations, consultez Configurer CloudFront pour transférer l'`en-tête` d'autorisation.

Vous pouvez utiliser HTTP ou HTTPS pour transmettre les demandes à votre serveur d'origine. Pour plus d'informations, consultez Utilisez le protocole HTTPS avec CloudFront.

Durée de conservation dans le cache et durée de vie minimale

Pour contrôler la durée pendant laquelle vos objets restent en CloudFront cache avant de CloudFront transmettre une autre demande à votre origine, vous pouvez :

- Configurer votre origine pour ajouter un `Cache-Control` ou un champ d'en-tête `Expires` à chaque objet.
- Spécifiez une valeur pour le TTL minimum dans les comportements CloudFront du cache.
- Utiliser la valeur par défaut de 24 heures.

Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Adresses IP client

Si un utilisateur envoie une demande à CloudFront et n'inclut pas d'en-tête de `X-Forwarded-For` demande, CloudFront il obtient son adresse IP à partir de la connexion TCP, ajoute un `X-Forwarded-For` en-tête qui inclut l'adresse IP et transmet la demande à l'origine. Par exemple, si CloudFront extrait l'adresse IP `192.0.2.2` de la connexion TCP, il transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.2
```

Si un utilisateur envoie une demande à CloudFront et inclut un en-tête de `X-Forwarded-For` demande, CloudFront obtient l'adresse IP du spectateur à partir de la connexion TCP, l'ajoute à la fin de l'`X-Forwarded-For`en-tête et transmet la demande à l'origine. Par exemple, si la demande du spectateur inclut `X-Forwarded-For: 192.0.2.4,192.0.2.3` et CloudFront obtient l'adresse IP `192.0.2.2` de la connexion TCP, elle transmet l'en-tête suivant à l'origine :

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

Certaines applications, telles que les équilibreurs de charge (y compris Elastic Load Balancing), les pare-feux d'applications Web, les proxys inverses, les systèmes de prévention des intrusions et API Gateway, ajoutent l'adresse IP du serveur CloudFront périphérique qui a transmis la demande à la fin de l'en-tête. `X-Forwarded-For` Par exemple, si elle est CloudFront incluse `X-Forwarded-For:`

`192.0.2.2` dans une demande qu'elle transmet à ELB et si l'adresse IP du serveur CloudFront Edge est 192.0.2.199, la demande que reçoit votre instance EC2 contient l'en-tête suivant :

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> L'en-tête `X-Forwarded-For` contient les adresses IPv4 (par exemple, 192.0.2.44) et les adresses IPv6 (par exemple, 2001:0db8:85a3::8a2e:0370:7334).
> Lorsque vous analysez les adresses IPv6 dans l'`X-Forwarded-For`en-tête, utilisez des bibliothèques d'analyse d'adresses IP standard capables de gérer n'importe quel format IPv6 RFC 4291 valide.
> Notez également que l'`X-Forwarded-For`en-tête peut être modifié par chaque nœud sur le chemin vers le serveur actuel (CloudFront). Pour plus d'informations, consultez la section 8.1 de la RFC 7239. Vous pouvez également modifier l'en-tête à l'aide des fonctions de calcul CloudFront Edge.

Client-side Authentification SSL

CloudFront prend en charge l'authentification TLS mutuelle (mTLS) où le client et le serveur s'authentifient mutuellement à l'aide de certificats. Une fois mTLS configuré, CloudFront vous pouvez valider les certificats clients lors de la prise de contact TLS et éventuellement exécuter des CloudFront fonctions pour implémenter une logique de validation personnalisée.

Pour les origines qui demandent des certificats côté client lorsque mTLS n'est pas configuré, la demande est supprimée CloudFront .

Pour plus d'informations sur la configuration de mTLS, consultez???.

CloudFront ne prend pas en charge l'authentification des clients à l'aide de certificats SSL côté client. Si une origine demande un certificat côté client, la demande est CloudFront supprimée.

Compression

Pour plus d'informations, consultez Diffusion de fichiers compressés.

Demandes conditionnelles

Lorsqu'il CloudFront reçoit une demande concernant un objet qui a expiré depuis un cache périphérique, il transmet la demande à l'origine soit pour obtenir la dernière version de l'objet, soit

pour obtenir la confirmation de l'origine que le cache CloudFront périphérique possède déjà la dernière version. Généralement, lorsque l'origine a envoyé l'objet pour la dernière fois CloudFront, elle a inclus une `ETag` valeur, une `LastModified` valeur ou les deux valeurs dans la réponse. Dans la nouvelle demande qui est CloudFront transmise à l'origine, ajoutez CloudFront l'un des éléments suivants ou les deux :

- Un en-tête `If-Match` ou `If-None-Match` qui contient la valeur `ETag` pour la version expirée de l'objet.
- Un en-tête `If-Modified-Since` qui contient la valeur `LastModified` pour la version expirée de l'objet.

L'origine utilise ces informations pour déterminer si l'objet a été mis à jour et, par conséquent, s'il faut renvoyer l'objet entier CloudFront ou uniquement un code d'état HTTP 304 (non modifié).

> **Note**
>
> `If-Modified-Since`et les requêtes `If-None-Match` conditionnelles ne sont pas prises en charge lorsqu'il CloudFront est configuré pour transférer les cookies (tous ou un sous-ensemble).
> Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.

Cookies

Vous pouvez configurer CloudFront pour transférer les cookies vers votre source. Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.

Cross-origin partage de ressources (CORS)

Si vous souhaitez CloudFront respecter les paramètres de partage des ressources entre origines, configurez CloudFront pour transférer l'`Origin`en-tête vers votre origine. Pour plus d'informations, consultez Mise en cache de contenu basée sur des en-têtes de demandes.

Chiffrement

Vous pouvez demander aux spectateurs d'utiliser le protocole HTTPS pour envoyer des demandes CloudFront à votre origine personnalisée CloudFront et de transmettre les demandes à votre origine personnalisée en utilisant le protocole utilisé par l'observateur. Pour plus d'informations, consultez les paramètres de distribution suivants :

- Viewer Protocol Policy
- Protocole (origines personnalisées uniquement)

CloudFront transmet les requêtes HTTPS au serveur d'origine à l'aide des protocoles SSLv3 TLSv1.0, TLSv1.1,TLSv1.2, et TLSv1.3 . Pour les origines personnalisées, vous pouvez choisir les protocoles SSL que vous CloudFront souhaitez utiliser pour communiquer avec votre origine :

- Si vous utilisez la CloudFront console, choisissez les protocoles à l'aide des cases à cocher Origin SSL Protocols. Pour plus d'informations, consultez Créer une distribution.
- Si vous utilisez l' CloudFront API, spécifiez les protocoles à l'aide de l'`OriginSslProtocols`élément. Pour plus d'informations, consultez OriginSslProtocols et consultez DistributionConfig le manuel Amazon CloudFront API Reference.

Si l'origine est un compartiment Amazon S3, la valeur par défaut CloudFront sera TLSv1.3.

> **Important**
>
> Les autres versions de SSL et TLS ne sont pas prises en charge.

Pour plus d'informations sur l'utilisation du protocole HTTPS avec CloudFront, consultezUtilisez le protocole HTTPS avec CloudFront. Pour obtenir la liste des chiffrements qui prennent CloudFront en charge la communication HTTPS entre les spectateurs et CloudFront, et entre CloudFront et votre origine, consultez. Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront

Demandes GET qui incluent un corps de texte

Si une `GET` demande d'utilisateur inclut un corps, CloudFront renvoie un code d'état HTTP 403 (Interdit) au visualiseur.

Méthodes HTTP

Si vous configurez CloudFront pour traiter toutes les méthodes HTTP qu'il prend en charge, CloudFront accepte les demandes suivantes des spectateurs et les transmet à votre origine personnalisée :

- `DELETE`
- `GET`

- `HEAD`
- `OPTIONS`
- `PATCH`
- `POST`
- `PUT`

CloudFront met toujours en cache les réponses `GET` et les `HEAD` demandes. Vous pouvez également configurer CloudFront pour mettre en cache les réponses aux `OPTIONS` demandes. CloudFront ne met pas en cache les réponses aux demandes utilisant les autres méthodes.

Pour plus d'informations sur la façon de configurer si votre origine personnalisée traite ces méthodes, consultez la documentation de votre origine.

> **Important**
>
> Si vous configurez CloudFront pour accepter et transmettre à votre origine toutes les méthodes HTTP prises CloudFront en charge, configurez votre serveur d'origine pour qu'il gère toutes les méthodes. Par exemple, si vous configurez CloudFront pour accepter et transférer ces méthodes parce que vous souhaitez les utiliser`POST`, vous devez configurer votre serveur d'origine pour qu'il gère les `DELETE` demandes de manière appropriée afin que les utilisateurs ne puissent pas supprimer les ressources que vous ne souhaitez pas qu'ils suppriment. Pour plus d'informations, consultez la documentation de votre serveur HTTP.

En-têtes et CloudFront comportement des requêtes HTTP (origines personnalisées et Amazon S3)

Le tableau suivant répertorie les en-têtes de requête HTTP que vous pouvez transmettre aux origines Amazon S3 et personnalisée (avec les exceptions qui sont notées). Pour chaque en-tête, le tableau comprend des informations sur les points suivants :

- CloudFront comportement si vous ne configurez pas CloudFront pour transmettre l'en-tête à votre origine, ce qui entraîne la mise CloudFront en cache de vos objets en fonction des valeurs d'en-tête.
- Si vous pouvez configurer la mise CloudFront en cache des objets en fonction des valeurs d'en-tête de cet en-tête.

Vous pouvez CloudFront configurer la mise en cache des objets en fonction des valeurs `User-Agent` des en-têtes `Date` et, mais nous ne le recommandons pas. Ces en-têtes ont de nombreuses valeurs possibles, et la mise en cache basée sur leurs valeurs entraînerait le transfert d'un plus grand nombre de demandes CloudFront vers votre origine.

Pour plus d'informations sur la mise en cache selon des valeurs d'en-tête, consultez Mise en cache de contenu basée sur des en-têtes de demandes.

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
Other-defined en-têtes	Paramètres de cache hérités : CloudFront redirige les en-têtes vers votre source.	Oui
`Accept`	CloudFront supprime l'en-tête.	Oui
`Accept-Charset`	CloudFront supprime l'en-tête.	Oui
`Accept-Encoding`	Si la valeur contient `gzip` ou `br`, CloudFront transmet un `Accept-Encoding` en-tête normalisé à votre origine. Pour plus d'informations, consultez Prise en charge de la compression et Diffusion de fichiers compressés.	Oui
`Accept-Language`	CloudFront supprime l'en-tête.	Oui

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`Authorization`	• `GET`et `HEAD` demandes : CloudFront supprime le champ `Authorization` d'en-tête avant de transmettre la demande à votre origine. • `OPTIONS`requêtes : CloudFront supprime le champ `Authorization` d'en-tête avant de transmettre la demande à votre origine si vous configurez CloudFront pour mettre en cache les réponses aux `OPTIONS` demandes. CloudFront transmet le champ `Authorization` d'en-tête à votre origine si vous ne configurez pas CloudFront pour mettre en cache les réponses aux requêtes OPTIONS. • `DELETE`, `PATCH``POST`, et `PUT` requêtes : CloudFront ne supprime pas le champ d'en-tête avant de transmettre la demande à votre origine.	Oui
`Cache-Control`	CloudFront redirige l'en-tête vers votre origine.	Non
`CloudFront-Forwarded-Proto`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du protocole de la demande.	Oui

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`CloudFront-Is-Desktop-Viewer`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.	Oui
`CloudFront-Is-Mobile-Viewer`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.	Oui
`CloudFront-Is-Tablet-Viewer`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.	Oui
`CloudFront-Viewer-Country`	CloudFront n'ajoute pas l'en-tête avant de transmettre la demande à votre origine.	Oui
`Connection`	CloudFront remplace cet en-tête par `Connection: Keep-Alive` avant de transmettre la demande à votre origine.	Non
`Content-Length`	CloudFront redirige l'en-tête vers votre origine.	Non

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`Content-MD5`	CloudFront redirige l'en-tête vers votre origine.	Oui
`Content-Type`	CloudFront redirige l'en-tête vers votre origine.	Oui
`Cookie`	Si vous configurez CloudFront pour transférer les cookies, le champ `Cookie` d'en-tête sera transmis à votre origine. Dans le cas contraire, CloudFront supprime le champ `Cookie` d'en-tête. Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.	Non
`Date`	CloudFront redirige l'en-tête vers votre origine.	Oui, mais non recommandé
`Expect`	CloudFront supprime l'en-tête.	Oui
`From`	CloudFront redirige l'en-tête vers votre origine.	Oui
`Host`	CloudFront définit la valeur au nom de domaine de l'origine qui est associé à l'objet demandé. Vous ne pouvez pas mettre en cache en fonction de l'en-tête Host pour Amazon S3 ou MediaStore Origins.	Oui (personnalisée) Non (S3 et MediaStore)

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`If-Match`	CloudFront redirige l'en-tête vers votre origine.	Oui
`If-Modified-Since`	CloudFront redirige l'en-tête vers votre origine.	Oui
`If-None-Match`	CloudFront redirige l'en-tête vers votre origine.	Oui
`If-Range`	CloudFront redirige l'en-tête vers votre origine.	Oui
`If-Unmodified-Since`	CloudFront redirige l'en-tête vers votre origine.	Oui
`Max-Forwards`	CloudFront redirige l'en-tête vers votre origine.	Non
`Origin`	CloudFront redirige l'en-tête vers votre origine.	Oui
`Pragma`	CloudFront redirige l'en-tête vers votre origine.	Non
`Proxy-Authenticate`	CloudFront supprime l'en-tête.	Non
`Proxy-Authorization`	CloudFront supprime l'en-tête.	Non
`Proxy-Connection`	CloudFront supprime l'en-tête.	Non

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`Range`	CloudFront redirige l'en-tête vers votre origine. Pour plus d'informations, consultez Comment CloudFront traite les demandes partielles pour un objet (range GETs).	Oui, par défaut
`Referer`	CloudFront supprime l'en-tête.	Oui
`Request-Range`	CloudFront redirige l'en-tête vers votre origine.	Non
`TE`	CloudFront supprime l'en-tête.	Non
`Trailer`	CloudFront supprime l'en-tête.	Non
`Transfer-Encoding`	CloudFront redirige l'en-tête vers votre origine.	Non
`Upgrade`	CloudFront supprime l'en-tête, sauf si vous avez établi une WebSocket connexion.	Non (sauf pour les WebSocket connexions)

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d’en-tête est prise en charge
`User-Agent`	CloudFront remplace la valeur de ce champ d'en-tête par`Amazon CloudFront` . Si vous souhaitez CloudFront mettre en cache votre contenu en fonction de l'appareil utilisé par l'utilisateur, consultezConfiguration de la mise en cache en fonction du type d’appareil.	Oui, mais non recommandé
`Via`	CloudFront redirige l'en-tête vers votre origine.	Oui
`Warning`	CloudFront redirige l'en-tête vers votre origine.	Oui
`X-Amz-Cf-Id`	CloudFront ajoute l'en-tête à la demande de l'utilisateur avant de transmettre la demande à votre origine. La valeur d’en-tête contient une chaîne chiffrée qui identifie de façon unique la demande.	Non
`X-Edge-*`	CloudFront supprime tous les `X-Edge-*` en-têtes.	Non
`X-Forwarded-For`	CloudFront redirige l'en-tête vers votre origine. Pour plus d’informations, consultez Adresses IP client.	Oui
`X-Forwarded-Proto`	CloudFront supprime l'en-tête.	Non

En-tête	Comportement si vous ne configurez pas CloudFront la mise en cache en fonction des valeurs d'en-tête	La mise en cache en fonction de valeurs d'en-tête est prise en charge
`X-HTTP-Method-Override`	CloudFront supprime l'en-tête.	Oui
`X-Real-IP`	CloudFront supprime l'en-tête.	Non

Version de HTTP

CloudFront transmet les demandes à votre origine personnalisée en utilisant HTTP/1.1.

Longueur maximale d'une demande et longueur maximale d'une URL

La longueur maximale d'une demande, y compris le chemin, la chaîne de requête (le cas échéant) et les en-têtes, est de 32 768 octets.

CloudFront construit une URL à partir de la demande. La longueur maximale de cette URL est de 8 192 caractères.

Si une URL dépasse la longueur maximale, CloudFront renvoie le code d'état HTTP 414 (URI trop long) à l'utilisateur. Si une demande dépasse la longueur maximale parce que la taille de l'en-tête est dépassée, CloudFront renvoie le code d'état HTTP 494 au visualiseur. Dans les deux cas, met CloudFront fin à la connexion TCP avec le visualiseur.

OCSP Stapling

Lorsqu'un utilisateur soumet une demande HTTPS pour un objet, l'un CloudFront ou l'autre doit confirmer auprès de l'autorité de certification (CA) que le certificat SSL du domaine n'a pas été révoqué. L'agrafage OCSP accélère la validation des certificats en permettant de valider le certificat et de CloudFront mettre en cache la réponse de l'autorité de certification, de sorte que le client n'a pas besoin de valider le certificat directement auprès de l'autorité de certification.

L'amélioration des performances d'OCSP Stapling est plus prononcée lorsque CloudFront reçoit de nombreuses requêtes HTTPS pour des objets dans le même domaine. Chaque serveur situé dans un emplacement CloudFront périphérique doit soumettre une demande de validation distincte. Lorsque CloudFront reçoit de nombreuses requêtes HTTPS pour le même domaine, chaque serveur dans l'emplacement périphérique reçoit rapidement une réponse de l'autorité de certification qu'il peut « agrafer » (staple) dans un paquet de l'établissement de la liaison SSL ; lorsque l'utilisateur a vérifié que le certificat est valide, CloudFront peut servir l'objet demandé. Si votre distribution ne reçoit pas beaucoup de trafic dans un emplacement CloudFront périphérique, les nouvelles demandes sont plus susceptibles d'être dirigées vers un serveur qui n'a pas encore validé le certificat auprès de l'autorité de certification. Dans ce cas, le visualiseur exécute séparément l'étape de validation et le CloudFront serveur sert l'objet. Ce CloudFront serveur soumet également une demande de validation à l'autorité de certification, de sorte que la prochaine fois qu'il recevra une demande incluant le même nom de domaine, il recevra une réponse de validation de la part de l'autorité de certification.

Connexions persistantes

Lorsque CloudFront reçoit une réponse de votre origine, il essaie de maintenir la connexion pendant plusieurs secondes au cas où une autre demande arriverait pendant cette période. Maintenir une connexion persistante permet de gagner le temps requis pour ré-établir la connexion TCP et établir une autre liaison TLS pour les demandes ultérieures.

Pour plus d’informations, y compris sur la manière de configurer la durée des connexions persistantes, consultez Keep-alive délai d'expiration (origines personnalisées et VPC uniquement) dans la section Référence de tous les paramètres de distribution.

Protocoles

CloudFront transmet les requêtes HTTP ou HTTPS au serveur d'origine en fonction des critères suivants :

- Protocole de la demande à laquelle le spectateur envoie CloudFront, HTTP ou HTTPS.
- La valeur du champ Origin Protocol Policy dans la CloudFront console ou, si vous utilisez l' CloudFront API, l'`OriginProtocolPolicy`élément du type `DistributionConfig` complexe. Dans la CloudFront console, les options sont HTTP uniquement, HTTPS uniquement et Match Viewer.

Si vous spécifiez HTTP uniquement ou HTTPS uniquement, CloudFront transmet les demandes au serveur d'origine en utilisant le protocole spécifié, quel que soit le protocole utilisé dans la demande du visualiseur.

Si vous spécifiez Match Viewer, CloudFront transfère les demandes au serveur d'origine en utilisant le protocole indiqué dans la demande du visualiseur. Notez que CloudFront ne met l'objet en cache qu'une seule fois, même si les utilisateurs émettent des demandes à l'aide des protocoles HTTP et HTTPS.

> **Important**
>
> Il CloudFront transmet une demande à l'origine à l'aide du protocole HTTPS, et si le serveur d'origine renvoie un certificat non valide ou un certificat auto-signé, interrompt CloudFront la connexion TCP.

Pour plus d'informations sur la mise à jour d'une distribution à l'aide de la CloudFront console, consultezMettre à jour une distribution. Pour plus d'informations sur la mise à jour d'une distribution à l'aide de l' CloudFront API, UpdateDistribution consultez le manuel Amazon CloudFront API Reference.

Chaînes de requête

Vous pouvez configurer si les paramètres CloudFront de chaîne de requête sont transférés à votre origine. Pour plus d'informations, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête.

Délai d'attente et tentatives de connexion à l'origine

Le délai d'expiration de la connexion à l'origine est le nombre de secondes qui CloudFront s'écoulent lors de la tentative d'établissement d'une connexion avec l'origine.

Les tentatives de connexion à l'origine sont le nombre de CloudFront tentatives de connexion à l'origine.

Ensemble, ces paramètres déterminent la durée pendant CloudFront laquelle vous essayez de vous connecter à l'origine avant de basculer vers l'origine secondaire (dans le cas d'un groupe d'origine) ou de renvoyer une réponse d'erreur à l'utilisateur. Par défaut, CloudFront attend 30 secondes (3 tentatives de 10 secondes chacune) avant de tenter de se connecter à l'origine secondaire ou de

renvoyer une réponse d'erreur. Vous pouvez réduire ce délai en spécifiant moins de tentatives, un délai d'attente de connexion plus court, ou les deux.

Pour plus d'informations, consultez Contrôle des délais d'expiration et des tentatives de l'origine.

Délai de réponse de l'origine

Le délai de réponse de l'origine, également appelé délai d'attente des opérations de lecture depuis l'origine ou délai de demande à l'origine, s'applique aux deux valeurs suivantes :

- Durée, en secondes, qui CloudFront attend une réponse après avoir transféré une demande à l'origine.
- Durée, en secondes, qui s'écoule CloudFront entre la réception d'un paquet d'une réponse de l'origine et la réception du paquet suivant.

CloudFront le comportement dépend de la méthode HTTP de la requête du visualiseur :

- `GET`et `HEAD` demandes : si l'origine ne répond pas ou cesse de répondre dans le délai imparti, interrompt CloudFront la connexion. Si le nombre spécifié de tentatives de connexion à l'origine est supérieur à 1, CloudFront essaie à nouveau d'obtenir une réponse complète. CloudFront essaie jusqu'à 3 fois, selon la valeur du paramètre Tentatives de connexion d'origine. Si l'origine ne répond pas lors de la dernière tentative, CloudFront ne réessaie pas tant qu'il ne reçoit pas une autre demande de contenu sur la même origine.
- `DELETE`,`OPTIONS`, `PATCH`PUT, et `POST` requêtes : si l'origine ne répond pas pendant la durée du délai de lecture, interrompt CloudFront la connexion et n'essaie pas à nouveau de contacter l'origine. Le client peut soumettre à nouveau la demande si nécessaire.

Pour plus d'informations, y compris sur la manière de configurer le délai de réponse de l'origine, consultez Délai de réponse.

Demandes simultanées pour le même objet (réduction des demandes)

Lorsqu'un emplacement CloudFront périphérique reçoit une demande pour un objet et que l'objet n'est pas dans le cache ou que l'objet mis en cache a expiré, envoie CloudFront immédiatement la demande à l'origine. Toutefois, s'il existe des demandes simultanées pour le même objet, c'est-à-dire si des demandes supplémentaires pour le même objet (avec la même clé de cache) arrivent à l'emplacement périphérique avant de CloudFront recevoir la réponse à la première demande,

CloudFront une pause s'arrête avant de transmettre les demandes supplémentaires à l'origine. Cette brève pause permet de réduire la charge sur l'origine. CloudFront envoie la réponse de la demande d'origine à toutes les demandes qu'il a reçues pendant sa pause. Ce processus se nomme la réduction des demandes. Dans CloudFront les journaux, la première demande est identifiée comme un `Miss` dans le `x-edge-result-type` champ, et les demandes réduites sont identifiées comme un`Hit`. Pour plus d'informations sur CloudFront les journaux, consultezthe section called "CloudFront et journalisation des fonctions Edge".

CloudFront réduit uniquement les requêtes qui partagent une clé de cache. Si les demandes supplémentaires ne partagent pas la même clé de cache parce que, par exemple, vous avez configuré CloudFront la mise en cache en fonction des en-têtes de demande, des cookies ou des chaînes de requête, CloudFront toutes les demandes avec une clé de cache unique sont transmises à votre origine.

Si vous souhaitez empêcher la fusion des demandes, vous pouvez utiliser la politique de cache gérée `CachingDisabled`, qui empêche également la mise en cache. Pour plus d'informations, consultez Utilisation des politiques de cache gérées.

Si vous souhaitez empêcher la fusion des demandes pour certains objets, vous pouvez définir la durée de vie minimale pour le comportement du cache sur 0 et configurer l'origine de sorte à envoyer `Cache-Control: private`, `Cache-Control: no-store`, `Cache-Control: no-cache`, `Cache-Control: max-age=0` ou `Cache-Control: s-maxage=0`. Ces configurations augmenteront la charge sur votre origine et introduiront une latence supplémentaire pour les demandes simultanées qui sont suspendues pendant l' CloudFront attente de la réponse à la première demande.

En-tête **`User-Agent`**

Si vous souhaitez CloudFront mettre en cache différentes versions de vos objets en fonction de l'appareil qu'un utilisateur utilise pour afficher votre contenu, nous vous recommandons de configurer CloudFront pour transférer un ou plusieurs des en-têtes suivants vers votre origine personnalisée :

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

En fonction de la valeur de l'`User-Agent`en-tête, CloudFront définit la valeur de ces en-têtes à `true` ou `false` avant de transmettre la demande à votre origine. Si un appareil entre dans plusieurs catégories, plusieurs valeurs peuvent être `true`. Par exemple, pour certaines tablettes, CloudFront peut définir `CloudFront-Is-Mobile-Viewer` et `CloudFront-Is-Tablet-Viewer` sur `true`. Pour plus d'informations sur la configuration CloudFront de la mise en cache en fonction des en-têtes de demande, consultezMise en cache de contenu basée sur des en-têtes de demandes.

Vous pouvez CloudFront configurer la mise en cache des objets en fonction des valeurs de l'`User-Agent`en-tête, mais nous ne le recommandons pas. L'`User-Agent`en-tête a de nombreuses valeurs possibles, et la mise en cache basée sur ces valeurs entraînerait le transfert CloudFront d'un plus grand nombre de demandes vers votre origine.

Si vous ne configurez CloudFront pas la mise en cache des objets en fonction des valeurs de l'`User-AgentUser-Agent`en-tête, CloudFront ajoute un en-tête avec la valeur suivante avant de transmettre une demande à votre origine :

```
User-Agent = Amazon CloudFront
```

CloudFront ajoute cet en-tête, que la demande du visualiseur en contienne `User-Agent` ou non. Si la demande du visualiseur inclut un `User-Agent` en-tête, CloudFront supprimez-le.

Comment CloudFront traite les réponses provenant de votre origine personnalisée

Découvrez comment CloudFront traite les réponses provenant de votre origine personnalisée.

Table des matières

- 100 Continuer les réponses
- Mise en cache
- Requêtes annulées
- Négociation de contenu
- Cookies
- Connexions TCP annulées
- en-têtes de réponse HTTP qui CloudFront suppriment ou remplacent
- Taille de fichier maximale pouvant être mise en cache
- Origine non disponible

- Redirections
- En-tête Transfer-Encoding

`100 Continuer` les réponses

Votre origine ne peut pas envoyer plus d'une réponse 100-Continuer à CloudFront. Après la première réponse 100-Continue, CloudFront s'attend à une réponse HTTP 200 OK. Si votre origine envoie une autre réponse 100-Continue après la première, une erreur CloudFront sera renvoyée.

Mise en cache

- Assurez-vous que le serveur d'origine définit des valeurs valides et précises pour les champs `Last-Modified` d'en-tête `Date` et.
- CloudFront respecte normalement un `Cache-Control: no-cache` en-tête dans la réponse depuis l'origine. Pour une exception, consultez Demandes simultanées pour le même objet (réduction des demandes).

Requêtes annulées

Si un objet ne se trouve pas dans le cache périphérique et si un utilisateur met fin à une session (par exemple, ferme un navigateur) après avoir récupéré l'objet depuis votre origine mais avant de pouvoir livrer l'objet demandé, CloudFront ne CloudFront met pas l'objet en cache à l'emplacement périphérique.

Négociation de contenu

Si votre origine est renvoyée `Vary:*` dans la réponse, et si la valeur du TTL minimum pour le comportement de cache correspondant est `0`, CloudFront met l'objet en cache mais transmet chaque demande ultérieure concernant l'objet à l'origine pour confirmer que le cache contient la dernière version de l'objet. CloudFront n'inclut aucun en-tête conditionnel, tel que `If-None-Match` ou`If-Modified-Since`. Par conséquent, votre origine renvoie l'objet à CloudFront en réponse à chaque demande.

Si votre origine est `Vary:*` renvoyée dans la réponse et si la valeur du TTL minimum pour le comportement de cache correspondant est une autre valeur, CloudFront traite l'`Vary`en-tête comme décrit dansen-têtes de réponse HTTP qui CloudFront suppriment ou remplacent.

Cookies

Si vous activez les cookies pour un comportement de cache, et si l'origine renvoie des cookies avec un objet, met en CloudFront cache à la fois l'objet et les cookies. Notez que cela réduit la capacité de mise en cache pour un objet. Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.

Connexions TCP annulées

Si la connexion TCP entre CloudFront et votre origine est interrompue alors que votre origine renvoie un objet à CloudFront, le CloudFront comportement dépend du fait que votre origine ait inclus ou non un `Content-Length` en-tête dans la réponse :

- Content-Length en-tête : CloudFront renvoie l'objet au visualiseur au fur et à mesure qu'il récupère l'objet depuis votre origine. Toutefois, si la valeur de l'`Content-Length`en-tête ne correspond pas à la taille de l'objet, celui-ci CloudFront ne sera pas mis en cache.
- Transfer-Encoding: Chunked : CloudFront renvoie l'objet au spectateur au fur et à mesure qu'il récupère l'objet depuis votre origine. Toutefois, si la réponse fragmentée n'est pas complète, l'objet CloudFront n'est pas mis en cache.
- Pas Content-Length d'en-tête : CloudFront renvoie l'objet au visualiseur et le met en cache, mais l'objet n'est peut-être pas complet. Sans en-tête `Content-Length`, CloudFront ne peut pas déterminer si la connexion TCP a été est annulée délibérément ou par erreur.

Nous vous recommandons de configurer votre serveur HTTP pour ajouter un `Content-Length` en-tête afin d' CloudFront empêcher la mise en cache d'objets partiels.

en-têtes de réponse HTTP qui CloudFront suppriment ou remplacent

CloudFront supprime ou met à jour les champs d'en-tête suivants avant de transmettre la réponse de votre origine au spectateur :

- `Set-Cookie`— Si vous configurez CloudFront pour transférer les cookies, le champ `Set-Cookie` d'en-tête sera transmis aux clients. Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.
- `Trailer`
- `Transfer-Encoding`— Si votre origine renvoie ce champ d'en-tête CloudFront , définissez la valeur sur `chunked` avant de renvoyer la réponse au spectateur.
- `Upgrade`

- `Vary` – Notez ce qui suit :
  - Si vous configurez CloudFront pour transférer l'un des en-têtes spécifiques à l'appareil vers votre origine (`CloudFront-Is-Desktop-Viewer`,, `CloudFront-Is-Mobile-ViewerCloudFront-Is-SmartTV-Viewer`,`CloudFront-Is-Tablet-Viewer`) et que vous configurez votre origine pour y `Vary:User-Agent` revenir CloudFront, le visualiseur est CloudFront `Vary:User-Agent` renvoyé. Pour plus d'informations, consultez Configuration de la mise en cache en fonction du type d'appareil.
  - Si vous configurez votre origine pour inclure l'une `Accept-Encoding` ou l'autre des valeurs `Cookie` dans l'`Vary`en-tête, CloudFront incluez les valeurs dans la réponse au visualiseur.
  - Si vous configurez CloudFront pour transférer les en-têtes vers votre origine, et si vous configurez votre origine pour renvoyer les noms des en-têtes qui se trouvent CloudFront dans l'`Vary`en-tête (par exemple,`Vary:Accept-Charset,Accept-Language`), CloudFront renvoie l'`Vary`en-tête avec ces valeurs au visualiseur.
  - Pour plus d'informations sur la façon dont CloudFront traite une valeur de `*` dans l'`Vary`en-tête, consultezNégociation de contenu.
  - Si vous configurez votre origine pour inclure d'autres valeurs dans l'`Vary`en-tête, CloudFront supprimez les valeurs avant de renvoyer la réponse au visualiseur.
- `Via`— CloudFront définit la valeur suivante dans la réponse au spectateur :

  ```
  Via: http-version alphanumeric-string.cloudfront.net (CloudFront)
  ```

  Par exemple, la valeur ressemble à ce qui suit :

  ```
  Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)
  ```

Taille de fichier maximale pouvant être mise en cache

La taille maximale d'un corps de réponse enregistré CloudFront dans son cache est de 50 Go. Cette taille inclut les réponses de transfert fragmentées qui ne spécifient pas la valeur d'en-tête `Content-Length`.

Vous pouvez CloudFront utiliser la mise en cache d'un objet dont la taille est supérieure à cette taille en utilisant des requêtes de plage pour demander les objets par parties de 50 Go ou moins chacune. CloudFrontmet ces parties en cache car chacune d'entre elles fait 50 Go ou moins. Une fois que l'utilisateur a récupéré toutes les parties de l'objet, il peut reconstruire l'objet d'origine plus large. Pour plus d'informations, consultez Utiliser les demandes de plage pour mettre en cache de large objets.

Origine non disponible

Si votre serveur d'origine n'est pas disponible et CloudFront reçoit une demande pour un objet qui se trouve dans le cache périphérique mais qui a expiré (par exemple, parce que la période spécifiée dans la `Cache-Control max-age` directive est écoulée), CloudFront soit diffuse la version expirée de l'objet, soit une page d'erreur personnalisée. Pour plus d'informations sur CloudFront le comportement lorsque vous avez configuré des pages d'erreur personnalisées, consultezComment CloudFront traiter les erreurs lorsque vous avez configuré des pages d'erreur personnalisées.

Dans certains cas, un objet rarement demandé est expulsé et n'est plus disponible dans le cache périphérique. CloudFront ne peut pas servir un objet qui a été expulsé.

Redirections

Si vous changez l'emplacement d'un objet sur le serveur d'origine, vous pouvez configurer votre serveur Web afin de rediriger les demandes vers le nouvel emplacement. Une fois que vous avez configuré la redirection, c'est la première fois qu'un utilisateur soumet une demande pour l'objet, CloudFront envoie la demande à l'origine, qui répond par une redirection (par exemple,`302 Moved Temporarily`). CloudFront met en cache la redirection et la renvoie à l'utilisateur. CloudFront ne suit pas la redirection.

Vous pouvez configurer votre serveur Web afin de rediriger les demandes vers l'un des emplacements suivants :

- La nouvelle URL de l'objet sur le serveur d'origine. Lorsque l'utilisateur suit la redirection vers la nouvelle URL, il la contourne CloudFront et revient directement à l'origine. Par conséquent, nous vous recommandons de ne pas rediriger des demandes vers la nouvelle URL de l'objet sur l'origine.
- La nouvelle CloudFront URL de l'objet. Lorsque le visualiseur soumet la demande contenant la nouvelle CloudFront URL, CloudFront récupère l'objet depuis le nouvel emplacement de votre origine, le met en cache à l'emplacement périphérique et renvoie l'objet au visualiseur. Les demandes suivantes pour l'objet seront servies par l'emplacement périphérique. Ceci évite la latence et la charge associées aux utilisateurs qui demandent l'objet à l'origine. Cependant, chaque nouvelle demande pour l'objet occasionne des frais pour deux demandes à CloudFront.

En-tête **`Transfer-Encoding`**

CloudFront prend uniquement en charge la `chunked` valeur de l'`Transfer-Encoding`en-tête. Si votre origine est renvoyée`Transfer-Encoding: chunked`, CloudFront renvoie l'objet au client

au fur et à mesure qu'il est reçu à l'emplacement périphérique, et met l'objet en cache au format fragmenté pour les demandes suivantes.

Si le visualiseur fait une `Range GET` demande et que l'origine revient`Transfer-Encoding: chunked`, CloudFront renvoie l'objet entier au visualiseur au lieu de la plage demandée.

Nous vous recommandons d'utiliser un encodage fragmenté si la longueur du contenu de votre réponse ne peut pas être prédéterminé. Pour plus d'informations, consultez Connexions TCP annulées.

Comportement des requêtes et des réponses pour les groupes d'origine

Les demandes adressées à un groupe d'origine fonctionnent de la même manière que celles d'une origine qui n'est pas configurée comme un groupe d'origine, sauf en cas de basculement d'origine. Comme pour toute autre origine, lorsque CloudFront reçoit une demande et que le contenu est déjà mis en cache dans un emplacement périphérique, le contenu est diffusé aux spectateurs depuis le cache. En l'absence de cache et lorsque l'origine est un groupe d'origine, les demandes de l'utilisateur sont transférées à l'origine principale dans le groupe d'origine.

Le comportement de demande et de réponse pour l'origine principale est le même que pour une origine qui n'est pas incluse dans un groupe d'origine. Pour plus d'informations, consultez Comportement des demandes et des réponses pour les origines Amazon S3 Origins et Comportement des demandes et des réponses pour les origines personnalisées.

La section suivante décrit le comportement du basculement d'origine lorsque l'origine principale renvoie des codes de statut HTTP spécifiques :

- Code d'état HTTP 2xx (succès) : CloudFront met le fichier en cache et le renvoie au visualiseur.
- Code d'état HTTP 3xx (redirection) : CloudFront renvoie le code d'état au visualiseur.
- Code d'état HTTP 4xx ou 5xx (client/server erreur) : si le code d'état renvoyé a été configuré pour le basculement, CloudFront envoie la même demande à l'origine secondaire du groupe d'origine.
- Code d'état HTTP 4xx ou 5xx (client/server erreur) : si le code d'état renvoyé n'a pas été configuré pour le basculement, CloudFront renvoie l'erreur au visualiseur.

CloudFront bascule vers l'origine secondaire uniquement lorsque la méthode HTTP de la demande du visualiseur est `GET`, `HEAD`, ou `OPTIONS`. CloudFront ne bascule pas lorsque l'utilisateur envoie une méthode HTTP différente (par exemple `POST`, `PUT`, et ainsi de suite).

Lors de l' CloudFront envoi d'une demande à une origine secondaire, le comportement de réponse est le même que pour une CloudFront origine qui ne fait pas partie d'un groupe d'origine.

Pour plus d'informations sur les groupes d'origine, consultez Optimisez la haute disponibilité grâce au basculement CloudFront d'origine.

Ajout d'en-têtes personnalisés aux demandes d'origine

Vous pouvez configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes qu'il envoie à votre origine. Les en-têtes personnalisés vous permettent d'envoyer et de récupérer des informations auprès de votre origine, données que les demandes d'utilisateur standard ne transmettent pas. Vous pouvez même personnaliser les en-têtes pour chaque origine. CloudFrontprend en charge les en-têtes personnalisés pour les origines personnalisées et les origines Amazon S3.

Table des matières

- Cas d'utilisation
- Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine
- En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine
- Configurer CloudFront pour transférer l'en-tête d'autorisation

Cas d'utilisation

Vous pouvez ajouter des en-têtes personnalisés, comme ceux présentés ci-dessous :

Identifier les demandes émanant de CloudFront

> Vous pouvez identifier les demandes que votre origine reçoit CloudFront. Cela peut être utile si vous voulez savoir si les utilisateurs CloudFront contournent ou si vous utilisez plusieurs CDN et que vous souhaitez obtenir des informations sur les demandes provenant de chaque CDN.

> **Note**
>
> Si vous utilisez une origine Amazon S3 avec journalisation des accès au serveur Amazon S3 activée, les journaux n'incluent pas les informations d'en-tête.

Détermination des demandes provenant d'une distribution particulière

Si vous configurez plusieurs CloudFront distributions pour utiliser la même origine, vous pouvez ajouter des en-têtes personnalisés différents dans chaque distribution. Vous pouvez alors utiliser les journaux de votre origine pour déterminer quelles demandes proviennent de quelle distribution CloudFront.

Activation du partage des ressources de plusieurs origines (CORS)

Si certains de vos spectateurs ne prennent pas en charge le partage de ressources entre origines (CORS), vous pouvez configurer CloudFront pour toujours ajouter l'`Origin`en-tête aux demandes qu'il envoie à votre origine. Ensuite, vous pouvez configurer votre origine pour renvoyer l'en-tête `Access-Control-Allow-Origin` pour chaque demande. Vous devez également configurer CloudFront pour respecter les paramètres CORS.

Contrôle de l'accès au contenu

Vous pouvez utiliser les en-têtes personnalisés pour contrôler l'accès au contenu. En configurant votre origine pour répondre aux demandes uniquement lorsqu'elles incluent un en-tête personnalisé ajouté par CloudFront, vous empêchez les utilisateurs de contourner votre contenu CloudFront et d'y accéder directement sur l'origine. Pour plus d’informations, consultez Restriction de l’accès à des fichiers d’origines personnalisées.

Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine

Pour configurer une distribution afin d'ajouter des en-têtes personnalisés aux demandes qu'elle envoie à votre origine, mettez à jour la configuration de l'origine via l'une des méthodes suivantes :

- CloudFront console — Lorsque vous créez ou mettez à jour une distribution, spécifiez les noms et les valeurs des en-têtes dans les paramètres Ajouter des en-têtes personnalisés. Pour plus d’informations, consultez Ajout d'en-tête personnalisé.

- CloudFront API : pour chaque origine à laquelle vous souhaitez ajouter des en-têtes personnalisés, spécifiez les noms et les valeurs des en-têtes dans le `CustomHeaders` champ qui s'y trouve`Origin`. Pour plus d'informations, consultez CreateDistribution ou consultez UpdateDistribution le manuel Amazon CloudFront API Reference.

Si les noms d'en-tête et les valeurs que vous spécifiez ne figurent pas déjà dans la demande de visualisation, CloudFront ajoutez-les à la demande d'origine. Si un en-tête est présent, CloudFront remplace la valeur de l'en-tête avant de transmettre la demande à l'origine.

Pour connaître les quotas qui s'appliquent aux en-têtes personnalisés d'origine, consultez Quotas sur les en-têtes.

En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine

Vous ne pouvez pas configurer CloudFront pour ajouter l'un des en-têtes suivants aux requêtes qu'il envoie à votre origine :

- `Cache-Control`
- `Connection`
- `Content-Length`
- `Cookie`
- `Host`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Range`
- `If-Unmodified-Since`
- `Max-Forwards`
- `Pragma`
- `Proxy-Authenticate`
- `Proxy-Authorization`
- `Proxy-Connection`
- `Range`

- `Request-Range`
- `TE`
- `Trailer`
- `Transfer-Encoding`
- `Upgrade`
- `Via`
- En-têtes commençant par `X-Amz-`
- En-têtes commençant par `X-Edge-`
- `X-Real-Ip`

Configurer CloudFront pour transférer l'**`en-tête`** d'autorisation

Lorsque CloudFront vous transférez une demande d'utilisateur à votre origine, CloudFront supprime certains en-têtes de visionnage par défaut, y compris l'`Authorization`en-tête. Pour vous assurer que votre origine reçoit toujours l'en-tête `Authorization` dans les demandes d'origine, vous disposez des options suivantes :

- Ajoutez l'en-tête `Authorization` à la clé de cache à l'aide d'une stratégie de cache. Tous les en-têtes de la clé de cache sont automatiquement inclus dans les demandes d'origine. Pour plus d'informations, consultez Contrôle de la clé de cache à l'aide d'une politique.
- Ajoutez l'`Authorization`en-tête individuellement dans une politique de demande d'origine. Pour plus d'informations, consultez Contrôle des demandes d'origine à l'aide d'une stratégie.
- Utilisez une politique de demande d'origine qui transmet tous les en-têtes de l'utilisateur à l'origine. CloudFront fournit une politique de demande d'origine gérée pour ce cas d'utilisation, appelée Managed-AllViewer. Pour plus d'informations, consultez Utilisation des stratégies de demande d'origine gérées.

> **Important**
>
> Si vous transférez l'`Authorization`en-tête vers votre origine sans l'inclure dans la clé de cache, assurez-vous que votre origine ne dépend pas de l'`Authorization`en-tête pour contrôler l'accès au contenu mis en cache. Lorsque l'`Authorization`en-tête ne fait pas partie de la clé de cache, CloudFront peut fournir la même réponse en cache aux spectateurs autorisés et non autorisés. Incluez l'`Authorization`en-tête dans la clé de cache à l'aide

d'une politique de cache ou désactivez complètement la mise en cache pour les origines qui nécessitent un traitement d'autorisation côté origine.

Comment CloudFront traite les demandes partielles pour un objet (range GETs)

Pour un objet large, l'utilisateur (navigateur web ou autre client) peut effectuer plusieurs demandes `GET` et utiliser l'en-tête de demande `Range` pour télécharger l'objet en parties plus petites. Ces demandes de plages d'octets, parfois appelées demandes `Range GET`, améliore l'efficacité des téléchargements partiels et la récupération de transferts ayant partiellement échoué.

Lorsqu'il CloudFront reçoit une `Range GET` demande, il vérifie le cache de l'emplacement périphérique qui a reçu la demande. Si le cache de cet emplacement périphérique contient déjà l'objet entier ou la partie demandée de l'objet, la plage demandée est CloudFront immédiatement distribuée depuis le cache.

Si le cache ne contient pas la plage demandée, CloudFront transmet la demande à l'origine. (Pour optimiser les performances, CloudFront vous pouvez demander une plage plus grande que celle demandée par le client dans le`Range GET`.) Ce qui se produit dépend de si l'origine prend en charge les demandes `Range GET` :

- Si l'origine prend en charge les **`Range GET`** requêtes, elle renvoie la plage demandée. CloudFront sert la plage demandée et la met également en cache pour les demandes futures. (Amazon S3 prend en charge les demandes `Range GET`, tout comme de nombreux serveurs HTTP.)
- Si l'origine ne prend pas en charge **`Range GET`** les requêtes, elle renvoie l'objet entier. CloudFront répond à la demande en cours en envoyant l'objet entier tout en le mettant en cache pour les demandes futures. Après avoir CloudFront mis en cache l'intégralité de l'objet dans un cache périphérique, il répond aux nouvelles `Range GET` demandes en diffusant la plage demandée.

Dans les deux cas, CloudFront commence à servir la plage ou l'objet demandé à l'utilisateur final dès que le premier octet arrive de l'origine.

> **Note**
>
> Si le visualiseur fait une `Range GET` demande et que l'origine revient`Transfer-Encoding: chunked`, CloudFront renvoie l'objet entier au visualiseur au lieu de la plage demandée.

CloudFront suit généralement la spécification RFC pour l'`Range`en-tête. Cependant si vos en-têtes `Range` ne respectent pas les exigences suivantes, CloudFront renvoie un code de statut HTTP `200` avec l'objet entier au lieu du code de statut `206` avec les plages spécifiées :

- Les plages doivent être répertoriées en ordre croissant. Par exemple, `100-200,300-400` est valide, mais pas `300-400,100-200`.
- Les plages ne doivent pas se chevaucher. Par exemple, `100-200,150-250` n'est pas valide.
- Toutes les spécifications de plages doivent être valides. Par exemple, vous ne pouvez pas spécifier une valeur négative dans une plage.

Pour plus d'informations sur l'en-tête de demande `Range`, consultez la section Demandes de plage dans RFC 7233, ou Plage dans MDN Web Docs.

Utiliser les demandes de plage pour mettre en cache de large objets

Lorsque la mise en cache est activée, CloudFront ne récupère ni ne met en cache un objet de plus de 50 Go. Lorsqu'une origine indique que l'objet est plus grand que cette taille (dans l'en-tête de `Content-Length` réponse), elle CloudFront ferme la connexion à l'origine et renvoie une erreur au visualiseur. (Lorsque la mise en cache est désactivée, CloudFront vous pouvez récupérer un objet dont la taille est supérieure à cette taille depuis l'origine et le transmettre au spectateur. Cependant, CloudFront ne met pas l'objet en cache.)

Cependant, avec les requêtes de plage, vous pouvez les utiliser CloudFront pour mettre en cache un objet dont la taille est supérieure à la taille de fichier maximale pouvant être mise en cache.

Example Exemple

1. Prenons l'exemple d'une origine contenant un objet de 100 Go. Lorsque la mise en cache est activée, CloudFront ne permet pas de récupérer ni de mettre en cache un objet de cette taille. Toutefois, l'utilisateur peut envoyer plusieurs demandes de plage pour récupérer cet objet par parties, chacune d'entre elles étant inférieure à 50 Go.

2. L’utilisateur peut demander l’objet dans des parties de 20 Go en envoyant une demande avec l’en-tête `Range: bytes=0-21474836480` pour récupérer la première partie, une autre demande avec l’en-tête `Range: bytes=21474836481-42949672960` pour récupérer la partie suivante, etc.
3. Lorsque l’utilisateur a reçu toutes les parties, il peut les combiner pour construire l’objet d’origine de 100 Go.
4. Dans ce cas, met en CloudFront cache chacune des parties de 20 Go de l'objet et peut répondre aux demandes ultérieures concernant la même partie depuis le cache.

Pour une demande de plage sur un objet compressé, la demande de plage d’octets se base sur la taille compressée, et non sur la taille originale de l’objet. Pour plus d’informations sur la compression des fichiers, consultez Diffusion de fichiers compressés.

Comment CloudFront traite les codes d'état HTTP 3xx depuis votre origine

Lorsque vous CloudFront demandez un objet à partir de votre compartiment Amazon S3 ou de votre serveur d'origine personnalisé, votre origine renvoie parfois un code d'état HTTP 3xx. Ce message indique généralement l’une des situations suivantes :

- L’URL de l’objet a changé (par exemple, les codes d’état 301, 302, 307 ou 308)
- L'objet n'a pas changé depuis la dernière fois que vous l'avez CloudFront demandé (code d'état 304)

CloudFront met en cache 3xx réponses en fonction des paramètres de votre CloudFront distribution et des en-têtes de la réponse. CloudFront met en cache 307 et 308 réponses uniquement lorsque vous incluez l'`Cache-Control`en-tête dans les réponses provenant de l'origine. Pour plus d’informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

Si votre origine renvoie un code d'état de redirection (par exemple, 301 ou 307), CloudFront elle ne suit pas la redirection. CloudFront transmet la réponse 301 ou 307 au spectateur, qui peut suivre la redirection en envoyant une nouvelle demande.

Comment CloudFront traite les codes d'état HTTP 4xx et 5xx depuis votre origine

Lorsque vous CloudFront demandez un objet à partir de votre compartiment Amazon S3 ou de votre serveur d'origine personnalisé, votre origine renvoie parfois un code d'état HTTP 4xx ou 5xx, ce qui indique qu'une erreur s'est produite. CloudFront le comportement dépend de :

- Si vous avez configuré des pages d’erreur personnalisées
- Si vous avez configuré la durée pendant laquelle vous souhaitez CloudFront mettre en cache les réponses d'erreur provenant de votre origine (TTL minimum de mise en cache des erreurs)
- Le code d’état
- Pour les codes d'état 5xx, si l'objet demandé se trouve actuellement dans le cache CloudFront périphérique
- Pour certains codes d’état 4xx, si l’origine renvoie un en-tête `Cache-Control max-age` ou `Cache-Control s-maxage`

CloudFront met toujours en cache les réponses `GET` et les `HEAD` demandes. Vous pouvez également configurer CloudFront pour mettre en cache les réponses aux `OPTIONS` demandes. CloudFront ne met pas en cache les réponses aux demandes utilisant les autres méthodes.

Si l'origine ne répond pas, la CloudFront demande à l'origine expire, ce qui est considéré comme une erreur HTTP 5xx provenant de l'origine, même si l'origine n'a pas répondu avec cette erreur. Dans ce scénario, CloudFront continue de diffuser du contenu mis en cache. Pour plus d’informations, consultez Origine non disponible.

Si vous avez activé la journalisation, CloudFront écrit les résultats dans les journaux quel que soit le code d'état HTTP.

Pour plus d'informations sur les fonctionnalités et les options liées au message d'erreur renvoyé par CloudFront, consultez les rubriques suivantes :

- Pour plus d'informations sur les paramètres des pages d'erreur personnalisées dans la CloudFront console, consultezPages d’erreur personnalisées et mise en cache des erreurs.
- Pour plus d'informations sur l'erreur lors de la mise en cache du TTL minimum dans la CloudFront console, consultez. Erreur de mise en cache de TTL minimum (secondes)

- Pour obtenir la liste des codes d'état HTTP mis en CloudFront cache, consultezCodes d'état HTTP 4xx et 5xx qui mettent en cache CloudFront.

Rubriques

- Comment CloudFront traiter les erreurs lorsque vous avez configuré des pages d'erreur personnalisées
- Comment traiter CloudFront les erreurs si vous n'avez pas configuré de pages d'erreur personnalisées
- Codes d'état HTTP 4xx et 5xx qui mettent en cache CloudFront

Comment CloudFront traiter les erreurs lorsque vous avez configuré des pages d'erreur personnalisées

Si vous avez configuré des pages d'erreur personnalisées, CloudFront le comportement dépend de la présence ou non de l'objet demandé dans le cache Edge.

L’objet demandé n’est pas dans le cache périphérique

CloudFront continue d'essayer d'obtenir l'objet demandé depuis votre origine lorsque toutes les conditions suivantes sont réunies :

- Un utilisateur demande un objet.
- L’objet n’est pas dans le cache périphérique.
- L’origine renvoie un code de statut HTTP 4xx ou 5xx et l’une des conditions suivantes est vraie :
  - L’origine renvoie un code de statut HTTP 5xx à la place d’un code de statut 304 (Non modifié) ou une version mise à jour de l’objet.
  - L’origine renvoie un code de statut HTTP 4xx qui n’est pas limité par un en-tête de contrôle de cache et est inclus dans la liste suivante de codes de statut: Codes d'état HTTP 4xx et 5xx qui mettent en cache CloudFront.
  - L’origine renvoie un code d’état HTTP 4xx sans en-tête `Cache-Control max-age` ou sans en-tête `Cache-Control s-maxage`, et le code d’état est inclus dans la liste suivante de codes d’état : Control Codes d'état HTTP 4xx qui mettent en CloudFront cache en fonction des en-têtes `Cache-Control`.

CloudFront effectue les opérations suivantes :

1. Dans le cache CloudFront périphérique qui a reçu la demande du lecteur, CloudFront vérifie votre configuration de distribution et obtient le chemin de la page d'erreur personnalisée qui correspond au code d'état renvoyé par votre origine.
2. CloudFront trouve le premier comportement de cache de votre distribution dont le modèle de chemin correspond au chemin de la page d'erreur personnalisée.
3. L'emplacement CloudFront périphérique envoie une demande pour la page d'erreur personnalisée à l'origine spécifiée dans le comportement du cache.
4. L'origine renvoie la page d'erreur personnalisée à l'emplacement périphérique.
5. CloudFront renvoie la page d'erreur personnalisée à l'utilisateur qui a fait la demande et met également en cache la page d'erreur personnalisée pour le maximum des valeurs suivantes :
   - La durée spécifiée par la durée de vie minimale (TTL) de la mise en cache des erreurs (10 secondes par défaut)
   - La durée spécifiée par un en-tête `Cache-Control max-age` ou un en-tête `Cache-Control s-maxage` qui est renvoyé par l'origine lorsque la première demande a généré l'erreur
6. Une fois le temps de mise en cache (déterminé à l'étape 5) écoulé, essayez à nouveau CloudFront d'obtenir l'objet demandé en transférant une autre demande à votre origine. CloudFront continue de réessayer aux intervalles spécifiés par le TTL minimum de mise en cache des erreurs.

> **Note**
>
> Si vous avez également configuré un comportement de cache pour la même page d'erreur personnalisée, CloudFront utilisez plutôt le comportement de cache TTL. Dans ce cas, CloudFront procédez comme suit pour les étapes 5 et 6 :
>
> - Après avoir CloudFront renvoyé la page d'erreur personnalisée au visualiseur qui a fait la demande, CloudFront vérifie le comportement du cache TTL (par exemple, vous définissez le TTL par défaut sur 5 secondes). CloudFront met ensuite en cache la page d'erreur personnalisée jusqu'à ce maximum.
> - Au bout de 5 secondes, CloudFront récupère à nouveau la page d'erreur personnalisée depuis l'origine. CloudFront continuera à réessayer à des intervalles spécifiés par le comportement du cache TTL.

Pour plus d'informations, consultez Paramètres de durée de vie du comportement de cache.

L'objet demandé est dans le cache périphérique

CloudFront continue de servir l'objet qui se trouve actuellement dans le cache Edge lorsque toutes les conditions suivantes sont réunies :

- Un utilisateur demande un objet.
- L'objet se trouve dans le cache périphérique, mais il a expiré
- L'origine renvoie un code de statut HTTP 5xx à la place d'un code de statut 304 (Non modifié) ou une version mise à jour de l'objet.

CloudFront effectue les opérations suivantes :

1. Si votre origine renvoie un code d'état 5xx, CloudFront sert l'objet même s'il est expiré. Pendant la durée de la mise en cache des erreurs, le TTL minimum CloudFront continue de répondre aux demandes des spectateurs en diffusant l'objet depuis le cache périphérique.

   Si votre origine renvoie un code de statut 4xx, CloudFront retourne le code de statut, et non l'objet demandé, à l'utilisateur.
2. Une fois le TTL minimum de mise en cache de l'erreur écoulé, essayez à nouveau CloudFront d'obtenir l'objet demandé en transférant une autre demande à votre origine. Notez que si l'objet n'est pas demandé fréquemment, il CloudFront peut être expulsé du cache périphérique alors que votre serveur d'origine renvoie toujours 5xx réponses. Pour plus d'informations sur la durée pendant laquelle les objets restent dans les caches CloudFront Edge, consultezGestion de la durée de conservation de contenu dans le cache (expiration).

Comment traiter CloudFront les erreurs si vous n'avez pas configuré de pages d'erreur personnalisées

Si vous n'avez pas configuré de pages d'erreur personnalisées, CloudFront le comportement dépend de la présence ou non de l'objet demandé dans le cache Edge.

Rubriques

- L’objet demandé n’est pas dans le cache périphérique
- L’objet demandé est dans le cache périphérique

L’objet demandé n’est pas dans le cache périphérique

CloudFront continue d'essayer d'obtenir l'objet demandé depuis votre origine lorsque toutes les conditions suivantes sont réunies :

- Un utilisateur demande un objet.
- L’objet n’est pas dans le cache périphérique.
- L’origine renvoie un code de statut HTTP 4xx ou 5xx et l’une des conditions suivantes est vraie :
  - L’origine renvoie un code de statut HTTP 5xx à la place d’un code de statut 304 (Non modifié) ou une version mise à jour de l’objet.
  - L’origine renvoie un code de statut HTTP 4xx qui n’est pas limité par un en-tête de contrôle de cache et est inclus dans la liste suivante de codes de statut: Codes d'état HTTP 4xx et 5xx qui mettent en cache CloudFront
  - L’origine renvoie un code d’état HTTP 4xx sans en-tête `Cache-Control max-age` ou sans en-tête `Cache-Control s-maxage`, et le code d’état est inclus dans la liste suivante de codes d’état : Control Codes d'état HTTP 4xx qui mettent en CloudFront cache en fonction des en-têtes `Cache-Control`.

CloudFront effectue les opérations suivantes :

1. CloudFront renvoie le code d'état 4xx ou 5xx à l'utilisateur et met également en cache le code d'état dans le cache périphérique qui a reçu la demande pour le maximum des valeurs suivantes :
   - La durée spécifiée par la durée de vie minimale (TTL) de la mise en cache des erreurs (10 secondes par défaut)
   - La durée spécifiée par un en-tête `Cache-Control max-age` ou un en-tête `Cache-Control s-maxage` qui est renvoyé par l’origine lorsque la première demande a généré l’erreur
2. Pendant la durée de mise en cache (déterminée à l'étape 1), CloudFront répond aux demandes d'utilisateur suivantes pour le même objet avec le code de statut 4xx ou 5xx mis en cache.
3. Une fois le temps de mise en cache (déterminé à l'étape 1) écoulé, essayez à nouveau CloudFront d'obtenir l'objet demandé en transférant une autre demande à votre origine. CloudFront continue de réessayer aux intervalles spécifiés par le TTL minimum de mise en cache des erreurs.

L’objet demandé est dans le cache périphérique

CloudFront continue de servir l'objet qui se trouve actuellement dans le cache Edge lorsque toutes les conditions suivantes sont réunies :

- Un utilisateur demande un objet.
- L’objet se trouve dans le cache périphérique, mais il a expiré Cela signifie que l’objet est obsolète.
- L’origine renvoie un code de statut HTTP 5xx à la place d’un code de statut 304 (Non modifié) ou une version mise à jour de l’objet.

CloudFront effectue les opérations suivantes :

1. Si votre origine renvoie un code d'erreur 5xx, CloudFront sert l'objet même s'il est expiré. Pendant la durée de la mise en cache des erreurs, le TTL minimum (10 secondes par défaut) CloudFront continue de répondre aux demandes des spectateurs en diffusant l'objet depuis le cache périphérique.

   Si votre origine renvoie un code de statut 4xx, CloudFront retourne le code de statut, et non l'objet demandé, à l'utilisateur.
2. Une fois le TTL minimum de mise en cache de l'erreur écoulé, essayez à nouveau CloudFront d'obtenir l'objet demandé en transférant une autre demande à votre origine. Si l'objet n'est pas demandé fréquemment, il CloudFront peut être expulsé du cache périphérique alors que votre serveur d'origine renvoie toujours 5xx réponses. Pour plus d’informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

> **Tip**
>
> - Si vous configurez la directive `stale-if-error` ou `Stale-While-Revalidate`, vous pouvez spécifier la durée pendant laquelle les objets obsolètes restent disponibles dans le cache périphérique. Ainsi, vous pouvez continuer à proposer du contenu à vos spectateurs même lorsque votre origine n'est pas disponible. Pour plus d’informations, consultez Diffusion de contenu obsolète (expiré).
> - CloudFront ne servira qu'un objet obsolète jusqu'à la valeur TTL ??? maximale spécifiée. Après cette durée, l’objet ne sera plus disponible dans le cache périphérique.

Codes d'état HTTP 4xx et 5xx qui mettent en cache CloudFront

CloudFront met en cache les codes d'état HTTP 4xx et 5xx renvoyés par votre origine, en fonction du code d'état spécifique renvoyé et du fait que votre origine renvoie des en-têtes spécifiques dans la réponse.

CloudFront met en cache les codes d'état HTTP 4xx et 5xx suivants renvoyés par votre origine. Si vous avez configuré une page d'erreur personnalisée pour un code d'état HTTP, la page d'erreur personnalisée est mise en CloudFront cache.

> **Note**
>
> Si vous utilisez la politique de cache CachingDisabled géré, ces codes d'état ou ces pages d'erreur personnalisées CloudFront ne seront pas mis en cache.

Code de statut HTTP	Description
404	Introuvable
414	Request-URI Trop grand
500	Erreur de serveur interne
501	Non implémenté
502	Passerelle erronée
503	Service non disponible
504	Passerelle Time-out

Codes d'état HTTP 4xx qui mettent en CloudFront cache en fonction des en-têtes `Cache-Control`

CloudFront met uniquement en cache les codes d'état HTTP 4xx suivants renvoyés par votre origine si votre origine renvoie un en-tête `Cache-Control max-age` ou`Cache-Control s-maxage`. Si vous avez configuré une page d'erreur personnalisée pour l'un de ces codes d'état HTTP et que votre origine renvoie l'un des en-têtes de contrôle du cache, la page d'erreur personnalisée est mise en CloudFront cache.

Code de statut HTTP	Description
400	Demande erronée
403	Accès interdit
405	Méthode non autorisée
412[1]	Échec de condition préalable
415[1]	Type de support non pris en charge

[1] CloudFront ne prend pas en charge la création de pages d'erreur personnalisées pour ces codes d'état HTTP.

Génération de réponses aux·erreurs personnalisées

Si un objet que vous diffusez n' CloudFront est pas disponible pour une raison quelconque, votre serveur Web renvoie généralement un code d'état HTTP pertinent CloudFront pour l'indiquer. Par exemple, si un utilisateur demande une URL non valide, votre serveur Web renvoie un code d'état HTTP 404 (Introuvable) à CloudFront, puis le CloudFront renvoie au lecteur. Au lieu d'utiliser cette réponse d'erreur par défaut, vous pouvez en créer une personnalisée qui sera CloudFront renvoyée au lecteur.

Si vous configurez CloudFront pour renvoyer une page d'erreur personnalisée pour un code d'état HTTP mais que la page d'erreur personnalisée n'est pas disponible, CloudFront renvoie au lecteur le code d'état CloudFront reçu de l'origine contenant les pages d'erreur personnalisées. Supposons, par exemple, que votre origine personnalisée renvoie un code de statut 500 et que vous ayez configuré CloudFront pour obtenir une page d'erreur personnalisée pour un code de statut 500 provenant d'un compartiment Amazon S3. Cependant, quelqu'un a accidentellement supprimé la page d'erreur personnalisée de votre compartiment Amazon S3. CloudFront renvoie un code d'état HTTP 404 (Not Found) au visualiseur qui a demandé l'objet.

Lorsque vous CloudFront renvoyez une page d'erreur personnalisée à un lecteur, vous payez les CloudFront frais standard pour la page d'erreur personnalisée, et non les frais pour l'objet demandé. Pour plus d'informations sur les CloudFront frais, consultez Amazon CloudFront Pricing.

Rubriques

- Configuration du comportement de réponses aux·erreurs
- Création d’une page d’erreur personnalisée pour des codes d’état HTTP spécifiques
- Stockage des objets et des pages d’erreur personnalisées dans des emplacements différents
- Modifier les codes de réponse renvoyés par CloudFront
- Contrôlez la durée de mise en CloudFront cache des erreurs

Configuration du comportement de réponses aux·erreurs

Plusieurs options s'offrent à vous pour gérer le CloudFront mode de réponse en cas d'erreur. Pour configurer des réponses d'erreur personnalisées, vous pouvez utiliser la CloudFront console, l' CloudFront API ou CloudFormation. Indépendamment de la façon dont vous choisissez de mettre à jour la configuration, tenez compte des conseils et recommandations suivants :

- Enregistrez vos pages d'erreur personnalisées dans un emplacement accessible à CloudFront. Nous vous recommandons de les stocker dans un compartiment Amazon S3 et de ne pas les stocker dans le même emplacement que le reste du contenu de votre site Web ou de votre application. Si vous stockez les pages d'erreur personnalisées sur la même origine que votre site Web ou votre application, et que l'origine commence à renvoyer des erreurs 5xx, CloudFront vous ne pouvez pas obtenir les pages d'erreur personnalisées car le serveur d'origine n'est pas disponible. Pour de plus amples informations, veuillez consulter Stockage des objets et des pages d’erreur personnalisées dans des emplacements différents.

- Assurez-vous qu'il CloudFront est autorisé à obtenir vos pages d'erreur personnalisées. Si les pages d'erreur personnalisées sont stockées dans Amazon S3, elles doivent être accessibles au public ou vous devez configurer un contrôle CloudFront d'accès à l'origine (OAC). Si les pages d'erreur personnalisées sont stockées dans une origine personnalisée, les pages doivent être accessibles publiquement.
- (Facultatif) Configurez votre origine de sorte qu'elle ajoute un en-tête `Cache-Control` ou `Expires` avec les pages d'erreur personnalisées, si vous le souhaitez. Vous pouvez également utiliser le paramètre TTL minimal de mise en cache des erreurs pour contrôler la durée de mise en cache CloudFront des pages d'erreur personnalisées. Pour de plus amples informations, veuillez consulter Contrôlez la durée de mise en CloudFront cache des erreurs.

Configuration de réponses aux·erreurs personnalisées

Pour configurer des réponses d'erreur personnalisées dans la CloudFront console, vous devez disposer d'une CloudFront distribution. Dans la console, les paramètres de configuration des réponses d'erreur personnalisées ne sont disponibles que pour les distributions existantes. Pour savoir comment créer une distribution, consultez Commencez avec une distribution CloudFront standard.

Console

Pour configurer des réponses d'erreur personnalisées (console)

1. Connectez-vous à la page Distributions Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#distributions.
2. Dans la liste des distributions, sélectionnez la distribution à mettre à jour.
3. Cliquez sur l'onglet Pages d'erreur, puis cliquez sur Créer une réponse d'erreur personnalisée.
4. Entrez les valeurs applicables. Pour de plus amples informations, veuillez consulter Pages d'erreur personnalisées et mise en cache des erreurs.
5. Après avoir saisi les valeurs souhaitées, cliquez sur Créer.

CloudFront API or CloudFormation

Pour configurer des réponses d'erreur personnalisées avec l' CloudFront API CloudFormation, utilisez le `CustomErrorResponse` type dans une distribution. Pour plus d'informations, consultez les ressources suivantes :

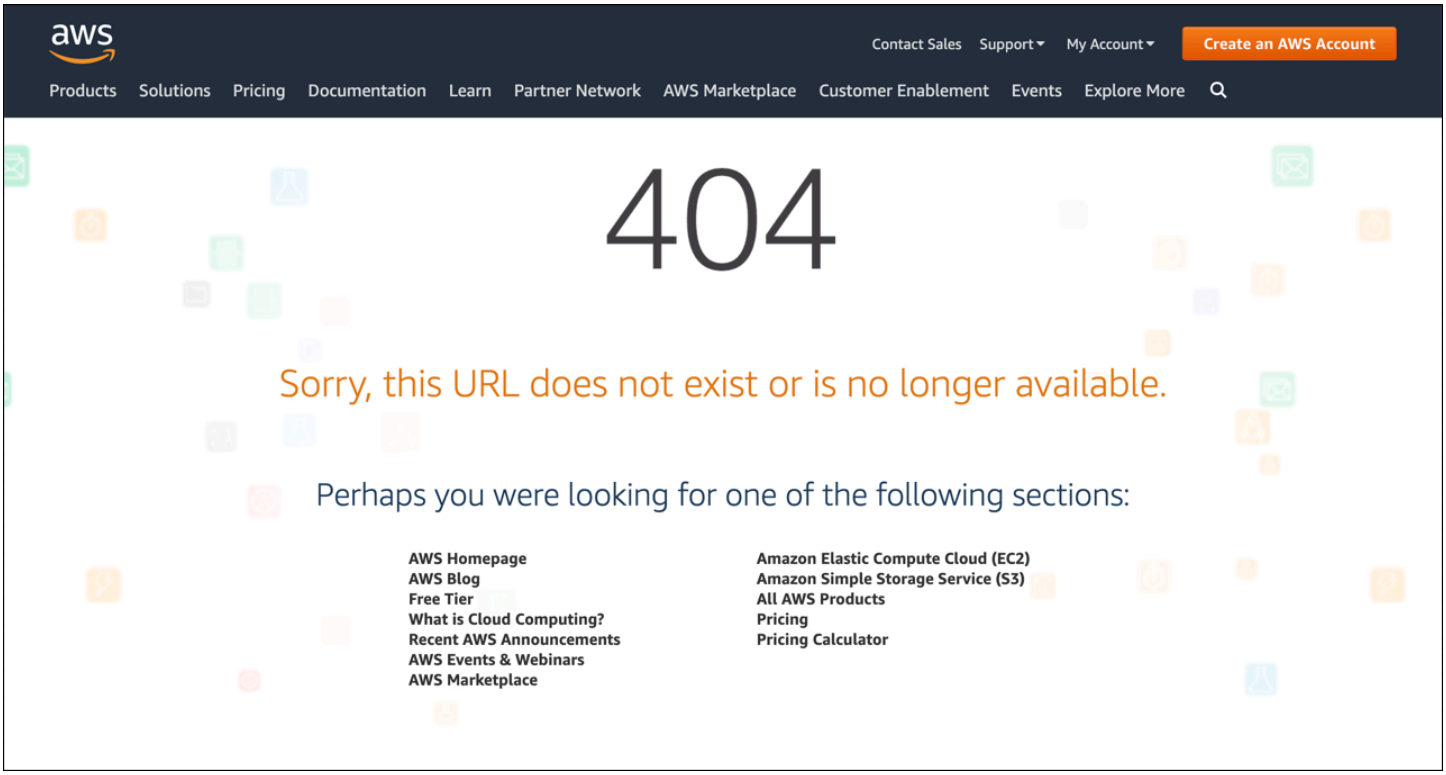
- AWS::CloudFront: :Distribution CustomErrorResponse dans le guide de l'AWS CloudFormation utilisateur
- CustomErrorResponsedans le Amazon CloudFront API Reference

Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques

Si vous préférez afficher un message d'erreur personnalisé au lieu du message par défaut (par exemple, une page qui utilise le même format que le reste de votre site Web), vous pouvez demander à l'utilisateur de CloudFront renvoyer un objet (tel qu'un fichier HTML) contenant votre message d'erreur personnalisé.

Pour spécifier le fichier que vous souhaitez renvoyer et les erreurs pour lesquelles le fichier doit être renvoyé, vous mettez à jour votre CloudFront distribution pour spécifier ces valeurs. Pour de plus amples informations, veuillez consulter Configuration du comportement de réponses aux·erreurs.

Par exemple, voici une page d'erreur personnalisée :



Vous pouvez spécifier un objet différent pour chaque code de statut HTTP pris en charge, ou utiliser le même objet pour tous les codes de statut pris en charge. Vous pouvez choisir de spécifier des pages d'erreur personnalisées pour certains codes d'état et pas d'autres.

Les objets que vous servez CloudFront peuvent être indisponibles pour diverses raisons. Ces raisons se divisent en deux grandes catégories :

- Les erreurs client indiquent un problème lié à la demande. Par exemple, un objet portant le nom spécifié n'est pas disponible, ou l'utilisateur ne dispose pas des autorisations requises pour obtenir un objet dans votre compartiment Amazon S3. Lorsqu'une erreur client se produit, l'origine renvoie un code d'état HTTP compris entre 4xx et. CloudFront
- Les erreurs serveur indiquent un problème lié au serveur d'origine. Par exemple, le serveur HTTP est occupé ou indisponible. Lorsqu'une erreur de serveur se produit, soit votre serveur d'origine renvoie un code d'état HTTP de l'ordre de 5xx à CloudFront, soit CloudFront il ne reçoit pas de réponse de votre serveur d'origine pendant un certain temps et suppose un code d'état 504 (Gateway Timeout).

Les codes d'état HTTP pour lesquels une page d'erreur personnalisée CloudFront peut être renvoyée sont les suivants :

- 400, 403, 404, 405, 414, 416
- 500, 501, 502, 503, 504

> **Remarques**
>
> - S'il CloudFront détecte que la demande n'est peut-être pas sûre, CloudFront renvoie une erreur 400 (mauvaise demande) au lieu d'une page d'erreur personnalisée.
> - Vous pouvez créer une page d'erreur personnalisée pour le code d'état HTTP 416 (plage demandée non satisfaisante), et vous pouvez modifier le code d'état HTTP qui est CloudFront renvoyé aux utilisateurs lorsque votre origine renvoie un code d'état 416 à CloudFront. Pour de plus amples informations, veuillez consulter Modifier les codes de réponse renvoyés par CloudFront. Cependant, CloudFront ne met pas en cache les réponses du code d'état 416, donc même si vous spécifiez une valeur pour Error Caching Minimum TTL pour le code d'état 416, CloudFront il ne l'utilise pas.
> - Dans certains cas, CloudFront ne renvoie pas de page d'erreur personnalisée pour le code d'état HTTP 503, même si vous le configurez CloudFront à cet effet. Si le code CloudFront d'erreur est `Capacity Exceeded` ou`Limit Exceeded`, CloudFront renvoie un code d'état 503 au lecteur sans utiliser votre page d'erreur personnalisée.
> - Si vous avez créé une page d'erreur personnalisée, elle CloudFront sera renvoyée `Connection: close` ou `Connection: keep-alive` pour les codes de réponse suivants :
>   - CloudFront retours `Connection: close` pour les codes d'état : 400, 405, 414, 416, 500, 501
>   - CloudFront retours `Connection: keep-alive` pour les codes d'état : 403, 404, 502, 503, 504

Pour une explication détaillée de la gestion CloudFront des réponses d'erreur provenant de votre origine, consultezComment CloudFront traite les codes d'état HTTP 4xx et 5xx depuis votre origine.

Stockage des objets et des pages d’erreur personnalisées dans des emplacements différents

Si vous souhaitez stocker vos objets et vos pages d’erreur personnalisées dans des emplacements différents, votre distribution doit inclure un comportement de cache pour lequel les conditions suivantes sont vraies :

- La valeur de Modèle de chemin correspond au chemin d'accès de vos messages d'erreur personnalisés. Par exemple, supposons que vous ayez enregistré des pages d'erreur personnalisées pour les erreurs 4xx dans un compartiment Amazon S3 d'un répertoire nommé `/4xx-errors`. Votre distribution doit inclure un comportement de cache pour lequel le modèle de chemin transmet les demandes de vos pages d'erreur personnalisées vers cet emplacement (par exemple,, `/4xx-errors/*`.
- La valeur d'Origine spécifie la valeur d'ID d'origine pour l'origine qui contient vos pages d'erreur personnalisées.

Pour de plus amples informations, veuillez consulter Paramètres de comportement du cache.

Modifier les codes de réponse renvoyés par CloudFront

Vous pouvez configurer CloudFront pour renvoyer au lecteur un code d'état HTTP différent de celui CloudFront reçu de l'origine. Par exemple, si votre origine renvoie un code d'état 500 àCloudFront, vous souhaiterez peut-être CloudFront renvoyer une page d'erreur personnalisée et un code d'état 200 (OK) au lecteur. Il existe plusieurs raisons pour lesquelles vous souhaiterez peut-être CloudFront renvoyer au spectateur un code de statut différent de celui renvoyé par votre source d'origine CloudFront :

- Certains dispositifs Internet (certains pare-feu et proxys d'entreprise, par exemple) interceptent les codes d'état HTTP 4xx et 5xx, et empêchent le renvoi d'une réponse à l'utilisateur. Dans ce cas, si vous remplacez `200`, la réponse n'est pas interceptée.
- Si vous ne vous souciez pas de faire la distinction entre les différentes erreurs client ou serveur, vous pouvez spécifier `400` ou `500` comme valeur CloudFront renvoyée pour tous les codes d'état 4xx ou 5xx.
- Vous pouvez décider de renvoyer un code d'état `200` (OK) et un site Web statique pour que vos clients ne sachent pas que votre site Web est en panne.

Si vous activez les journaux CloudFront standard et que vous configurez CloudFront pour modifier le code d'état HTTP dans la réponse, la valeur de la `sc-status` colonne des journaux contient le code d'état que vous spécifiez. Cela n'affecte pas la valeur de la colonne `x-edge-result-type`. Elle contient le type de résultat de la réponse de l'origine. Supposons, par exemple, que vous configuriez CloudFront pour renvoyer un code d'état de `200` au visualiseur lorsque l'origine renvoie `404` (Non trouvé) à CloudFront. Lorsque l'origine répond à une demande avec un code d'état `404`, la valeur

de la colonne `sc-status` dans le journal sera `200`, mais la valeur de la colonne `x-edge-result-type` sera `Error`.

Vous pouvez configurer CloudFront pour renvoyer l'un des codes d'état HTTP suivants ainsi qu'une page d'erreur personnalisée :

- 200
- 400, 403, 404, 405, 414, 416
- 500, 501, 502, 503, 504

Contrôlez la durée de mise en CloudFront cache des erreurs

CloudFront met en cache les réponses aux erreurs pendant une durée par défaut de 10 secondes. CloudFront soumet ensuite la demande suivante pour l'objet à votre origine pour voir si le problème à l'origine de l'erreur a été résolu et si l'objet demandé est disponible.

Vous pouvez spécifier la durée de mise en cache des erreurs (TTL minimum de mise en cache des erreurs) pour chaque code d'état 4xx et 5xx mis en cache. CloudFront (Pour plus d’informations, consultez Codes d'état HTTP 4xx et 5xx qui mettent en cache CloudFront.) Lorsque vous spécifiez une durée, veuillez noter les points suivants :

- Si vous spécifiez une courte durée de mise en cache des erreurs, CloudFront vous transmettez plus de demandes à votre origine que si vous spécifiez une durée plus longue. Pour les erreurs 5xx, cela peut aggraver le problème qui a initialement amené votre origine à renvoyer une erreur.
- Lorsque votre origine renvoie une erreur pour un objet, elle CloudFront répond aux demandes concernant l'objet soit par la réponse d'erreur, soit par votre page d'erreur personnalisée jusqu'à ce que la durée de mise en cache des erreurs soit écoulée. Si vous spécifiez une longue durée de mise en cache des erreurs, vous CloudFront pouvez continuer à répondre aux demandes avec une réponse d'erreur ou votre page d'erreur personnalisée pendant une longue période une fois que l'objet sera de nouveau disponible.

> **Note**
>
> Vous pouvez créer une page d'erreur personnalisée pour le code de statut HTTP 416 (Plage demandée impossible à respecter), et vous pouvez modifier le code de statut HTTP que CloudFront renvoie aux utilisateurs quand votre origine retourne un code de statut 416 à CloudFront. (Pour plus d’informations, consultez Modifier les codes de réponse renvoyés par

CloudFront.) Cependant, CloudFront ne met pas en cache les réponses du code d'état 416, donc même si vous spécifiez une valeur pour Error Caching Minimum TTL pour le code d'état 416, CloudFront il ne l'utilise pas.

Si vous souhaitez contrôler la durée de mise en CloudFront cache des erreurs pour des objets individuels, vous pouvez configurer votre serveur d'origine pour ajouter l'en-tête applicable à la réponse d'erreur pour cet objet.

Si l'origine ajoute une `Cache-Control: s-maxage` directive `Cache-Control: max-age` ou, ou un `Expires` en-tête, met en CloudFront cache les réponses d'erreur pour la valeur la plus élevée entre la valeur de l'en-tête ou le TTL minimal de mise en cache des erreurs.

Note

Les valeurs `Cache-Control: max-age` et `Cache-Control: s-maxage` ne peuvent pas être supérieures à la valeur de Maximum TTL (Durée de vie maximale) définie pour le comportement de cache pour lequel la page d'erreur est récupérée.

Si l'origine ajoute une `Cache-Control: private` directive `Cache-Control: no-storeCache-Control: no-cache`, ou pour les codes d'erreur 404, 410, 414 ou 501, la réponse d'erreur CloudFront ne sera pas mise en cache. Pour tous les autres codes d'erreur, CloudFront ignore les `private` directives `no-storeno-cache`, et met en cache la réponse d'erreur correspondant à la valeur du TTL minimal de mise en cache d'erreur.

Si l'origine ajoute d'autres `Cache-Control` directives ou n'ajoute aucun en-tête, CloudFront met en cache les réponses d'erreur pour la valeur de Error Caching Minimum TTL.

Si le délai d'expiration d'un code d'état 4xx ou 5xx pour un objet est supérieur à votre attente, et que l'objet est à nouveau disponible, vous pouvez invalider le code de l'erreur mise en cache à l'aide de l'URL de l'objet demandé. Si votre origine renvoie une réponse d'erreur pour plusieurs objets, vous devez invalider chaque objet séparément. Pour en savoir plus sur l'invalidation d'objets, consultez Invalidation de fichiers pour supprimer du contenu.

Si la mise en cache est activée pour l'origine d'un compartiment S3 et que vous configurez un TTL de mise en cache d'erreur de 0 seconde dans votre CloudFront distribution, vous verrez toujours un TTL de mise en cache d'une seconde pour les erreurs d'origine S3. CloudFront fait cela pour protéger votre origine contre les attaques DDoS. Cette règle ne concerne pas les autres types d’origines.

Ajouter, supprimer ou remplacer le contenu qui CloudFront distribue

Cette section explique comment vous assurer que vous CloudFront pouvez accéder au contenu que vous souhaitez proposer à vos spectateurs, comment spécifier les objets de votre site Web ou de votre application, et comment supprimer ou remplacer du contenu.

Rubriques

- Ajoutez du contenu diffusé et CloudFront accédez-y
- Utiliser le contrôle de version des fichiers pour mettre à jour ou supprimer du contenu d'une distribution CloudFront
- Personnalisez le format d'URL pour les fichiers dans CloudFront
- Spécification d’un objet racine par défaut
- Invalidation de fichiers pour supprimer du contenu
- Diffusion de fichiers compressés

Ajoutez du contenu diffusé et CloudFront accédez-y

Lorsque vous CloudFront souhaitez distribuer du contenu (objets), vous ajoutez des fichiers à l'une des origines que vous avez spécifiées pour la distribution et vous exposez un CloudFront lien vers les fichiers. Un emplacement CloudFront périphérique ne récupère pas les nouveaux fichiers depuis une origine tant que l'emplacement périphérique n'a pas reçu les demandes de l'utilisateur à leur sujet. Pour plus d’informations, consultez Comment CloudFront diffuse le contenu.

Lorsque vous ajoutez un fichier que vous CloudFront souhaitez distribuer, assurez-vous de l'ajouter à l'un des compartiments Amazon S3 spécifiés dans votre distribution ou, pour une origine personnalisée, à un répertoire du domaine spécifié. De plus vérifiez que le modèle de chemin dans le comportement de cache applicable envoie les demandes à l’origine correcte.

Par exemple, imaginons qu’un modèle de chemin pour un comportement de cache soit `*.html`. Si aucun autre comportement de cache n'est configuré pour réacheminer les requêtes vers cette origine, CloudFront réachemine uniquement les fichiers `*.html`. Dans ce scénario, par exemple, CloudFront ne distribuera jamais les fichiers .jpg que vous chargez sur l'origine, car vous n'avez pas encore créé de comportement de cache incluant les fichiers .jpg.

CloudFront les serveurs ne déterminent pas le type MIME des objets qu'ils desservent. Lorsque vous chargez un fichier dans votre origine, nous vous recommandons de définir le champ d'en-tête `Content-Type` pour celui-ci.

Utiliser le contrôle de version des fichiers pour mettre à jour ou supprimer du contenu d'une distribution CloudFront

Pour mettre à jour le contenu existant CloudFront configuré pour être distribué pour vous, nous vous recommandons d'utiliser un identifiant de version dans les noms de fichiers ou de dossiers. Cela vous permet de contrôler la gestion du contenu CloudFront diffusé.

Mise à jour des fichiers existants à l'aide de noms de fichiers versionnés

Lorsque vous mettez à jour des fichiers existants dans une CloudFront distribution, nous vous recommandons d'inclure une sorte d'identifiant de version dans vos noms de fichiers ou dans les noms de vos répertoires afin de mieux contrôler votre contenu. Cet identifiant peut être un horodatage, un numéro séquentiel ou toute autre méthode permettant de faire la distinction entre deux versions du même objet.

Par exemple, au lieu de nommer un fichier graphique image.jpg, vous pouvez l'appeler image_1.jpg. Lorsque vous souhaitez commencer à servir une nouvelle version du fichier, vous appellerez alors le nouveau fichier image_2.jpg et vous mettrez à jour les liens de votre application Web ou site Web pour pointer sur image_2.jpg. Sinon, vous pouvez placer tous les graphiques dans un répertoire images_v1, et lorsque vous souhaitez commencer à servir des nouvelles versions d'un ou plusieurs graphiques, vous créez un nouveau répertoire images_v2, et vous mettez à jour vos liens pour pointer sur ce répertoire. Grâce à la gestion des versions, vous n'avez pas à attendre l'expiration d'un objet pour CloudFront commencer à diffuser une nouvelle version de celui-ci, et vous n'avez pas à payer pour l'invalidation de l'objet.

Même si vous versionnez vos fichiers, nous vous recommandons de définir une date d'expiration. Pour plus d'informations, consultez Gestion de la durée de conservation de contenu dans le cache (expiration).

> **Note**
>
> La spécification de noms de fichier ou de répertoire versionnés n'est pas liée à la gestion des versions d'objets Amazon S3.

Supprimer du contenu pour CloudFront ne pas le diffuser

Vous pouvez supprimer des fichiers de votre origine que vous ne souhaitez plus voir inclus dans votre distribution CloudFront. Cependant, le contenu du cache Edge CloudFront continuera à être diffusé aux spectateurs jusqu'à l'expiration des fichiers.

Si vous souhaitez supprimer un fichier immédiatement, vous devez effectuer l'une des actions suivantes :

- Utilisez la gestion des versions de fichiers. Lorsque vous utilisez le versionnement, les différentes versions d'un fichier portent des noms différents que vous pouvez utiliser dans votre CloudFront distribution, afin de modifier le fichier qui est renvoyé aux utilisateurs. Pour plus d'informations, consultez Mise à jour des fichiers existants à l'aide de noms de fichiers versionnés.
- Invalidez le fichier. Pour plus d'informations, consultez Invalidation de fichiers pour supprimer du contenu.

Personnalisez le format d'URL pour les fichiers dans CloudFront

Après avoir configuré votre origine avec les objets (contenus) que vous souhaitez proposer CloudFront à vos spectateurs, vous devez utiliser les URL appropriées pour référencer ces objets dans le code de votre site Web ou de votre application afin de CloudFront pouvoir les diffuser.

Le nom de domaine que vous utilisez dans les URL pour les objets de vos pages web ou de votre application web peut être l'un des noms suivants :

- Le nom de domaine, tel que`d111111abcdef8.cloudfront.net`, qui est CloudFront automatiquement attribué lorsque vous créez une distribution
- Votre propre nom de domaine, comme `example.com`

Par exemple, vous pouvez utiliser l'une des URL suivantes pour renvoyer le fichier `image.jpg`:

```
https://d111111abcdef8.cloudfront.net/images/image.jpg
```

```
https://example.com/images/image.jpg
```

Vous utilisez le même format d'URL que vous stockiez le contenu dans des compartiments Amazon S3 ou dans une origine personnalisée, comme l'une de vos propres serveurs web.

> **Note**
>
> Le format d'URL dépend en partie de la valeur que vous spécifiez pour Chemin d'origine dans votre distribution. Cette valeur indique CloudFront le chemin du répertoire supérieur pour vos objets. Pour plus d'informations sur la définition du chemin d'accès d'origine lorsque vous créez une distribution, consultez Chemin d'origine.

Pour plus d'informations sur les formats d'URL, consultez les sections suivantes.

Utilisation de votre propre nom de domaine (exemple.com)

Au lieu d'utiliser le nom de domaine par défaut qui CloudFront vous est attribué lorsque vous créez une distribution, vous pouvez ajouter un autre nom de domaine plus facile à utiliser, par exemple`example.com`. En configurant votre propre nom de domaine avec CloudFront, vous pouvez utiliser une URL comme celle-ci pour les objets de votre distribution :

```
https://example.com/images/image.jpg
```

Si vous prévoyez d'utiliser le protocole HTTPS entre les spectateurs et CloudFront, consultezUtilisation de noms de domaines alternatifs et HTTPS.

Utilisation d'une barre oblique (/) à la fin dans des URL

Lorsque vous spécifiez des URL pour les annuaires de votre CloudFront distribution, choisissez de toujours utiliser une barre oblique finale ou de ne jamais utiliser de barre oblique finale. Par exemple, choisissez uniquement l'un des formats suivants pour toutes vos URL :

```
https://d111111abcdef8.cloudfront.net/images/
```

```
https://d111111abcdef8.cloudfront.net/images
```

Pourquoi est-ce important ?

Les deux formats permettent de créer des liens vers CloudFront des objets, mais la cohérence peut vous aider à éviter des problèmes lorsque vous souhaitez invalider un répertoire ultérieurement. CloudFront stocke les URL exactement telles qu'elles sont définies, y compris les barres obliques de fin. Ainsi, si votre format n'est pas cohérent, vous devrez invalider les URL des répertoires avec et sans barre oblique, pour vous assurer que cela CloudFront supprime le répertoire.

Ce n’est pas pratique d’invalider les deux formats d’URL et cela peut entraîner des coûts supplémentaires. En effet, si vous devez doubler les invalidations pour couvrir les deux types d’URL, vous risquez de dépasser le nombre maximum d’invalidations gratuites autorisées pour le mois. Et si tel est le cas, vous devrez payer pour toutes les invalidations, même s'il n'existe qu'un seul format pour chaque URL de répertoire dans CloudFront.

Création d’URL signées pour des contenus restreints

Si vous avez un contenu auquel vous souhaitez limiter l’accès, vous pouvez créer des URL signées. Par exemple, si vous voulez distribuer votre contenu uniquement aux utilisateurs qui se sont authentifiés, vous pouvez créer des URL qui sont valides uniquement pendant une période spécifiée ou qui sont disponibles uniquement à partir d’une adresse IP spécifiée. Pour plus d’informations, consultez Offre de contenu privé avec des URL et des cookies signés.

Spécification d’un objet racine par défaut

Vous pouvez configurer CloudFront pour renvoyer un objet spécifique (l'objet racine par défaut) lorsqu'un utilisateur (afficheur) demande l'URL racine de votre distribution au lieu de demander un objet dans votre distribution. Vous pouvez utiliser un objet racine par défaut pour éviter d’exposer le contenu de votre distribution.

Table des matières

- Comment spécifier un objet racine par défaut
- Fonctionnement de l'objet racine par défaut
- Comment CloudFront fonctionne si vous ne définissez pas d'objet racine

Comment spécifier un objet racine par défaut

Pour éviter d’exposer le contenu de votre distribution ou de renvoyer une erreur, spécifiez un objet racine par défaut pour votre distribution. Vous pouvez spécifier le nom exact du fichier ou le chemin d’accès au fichier. Par exemple, si votre objet racine est un fichier `index.html`, vous pouvez spécifier ce nom de fichier. Si votre fichier `index.html` se trouve dans un autre dossier, spécifiez plutôt le chemin, tel que *`exampleFolderName`*`/index.html`. Si vous définissez un chemin pour l’objet racine par défaut, les demandes des utilisateurs adressées à l’URL racine de la distribution renverront le fichier spécifié à partir de ce chemin. Vous pouvez utiliser un chemin de fichier pour disposer de plus de flexibilité dans l’organisation de votre contenu à l’origine, car votre objet racine par défaut peut se trouver dans un dossier plutôt qu’à la racine.

Pour spécifier un objet racine par défaut pour votre distribution

1. Chargez l’objet racine par défaut sur l’origine sur laquelle pointe votre distribution.

   Le fichier peut être de n'importe quel type pris en charge par CloudFront. Pour obtenir la liste des contraintes relatives au nom du fichier, consultez l'`DefaultRootObject`élément DistributionConfig du manuel Amazon CloudFront API Reference.

   > **Note**
   >
   > Si le nom de fichier de l'objet racine par défaut est trop long ou contient un caractère non valide, CloudFront renvoie l'erreur`HTTP 400 Bad Request - InvalidDefaultRootObject`. En outre, CloudFront met le code en cache pendant 10 secondes (par défaut) et écrit les résultats dans les journaux d'accès.

2. Vérifiez que les autorisations pour l'objet accordent au CloudFront moins un accès en lecture.

   Pour plus d’informations sur les autorisations Amazon S3, consultez Gestion des autorisations d’accès à vos ressources Amazon S3 dans le Guide du développeur Amazon Simple Storage Service.

3. Mettez à jour votre distribution pour faire référence à l'objet racine par défaut à l'aide de la CloudFront console ou de l' CloudFront API.

   Pour spécifier un objet racine par défaut à l'aide de la CloudFront console :

   a. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

   b. Dans le volet supérieur de la liste de distributions, sélectionnez la distribution à mettre à jour.

   c. Dans le volet Paramètres, sous l'onglet Général, choisissez Modifier.

   d. Dans la boîte de dialogue Modifier les paramètres, dans le champ Objet racine par défaut, entrez le nom de fichier ou le chemin de l’objet racine par défaut.

      > **Tip**
      >
      > Votre chaîne ne peut pas commencer par une barre oblique (`/`). Indiquez uniquement le nom de l’objet ou le chemin menant à cet objet. Par exemple, utilisez `index.html` ou *`exampleFolderName`*`/index.html`. Si vous spécifiez **/**

exampleFolderName/index.html ou /index.html, vous risquez d'obtenir une erreur 403 Accès refusé.

e. Cliquez sur Enregistrer les modifications.

Pour mettre à jour votre configuration à l'aide de l' CloudFront API, spécifiez une valeur pour l' DefaultRootObjectélément de votre distribution. Pour plus d'informations sur l'utilisation de l' CloudFront API pour spécifier un objet racine par défaut, consultez UpdateDistribution le manuel Amazon CloudFront API Reference.

4. Vérifiez que vous avez activé l'objet racine par défaut en demandant votre URL racine. Si votre navigateur n'affiche pas l'objet racine par défaut, effectuez les opérations suivantes :

   a. Vérifiez que votre distribution est entièrement déployée en consultant l'état de votre distribution sur la CloudFront console.

   b. Répétez les étapes 2 et 3 pour vérifier que vous avez accordé les autorisations correctes et que vous avez correctement mis à jour la configuration de votre distribution pour spécifier l'objet racine par défaut.

Fonctionnement de l'objet racine par défaut

Imaginons que la requête suivante pointe vers l'objet image.jpg:

```
https://d111111abcdef8.cloudfront.net/image.jpg
```

En revanche, la requête suivante pointe vers l'URL racine de la même distribution plutôt que sur un objet particulier, comme dans le premier exemple :

```
https://d111111abcdef8.cloudfront.net/
```

Lorsque vous définissez un objet racine par défaut, une demande d'utilisateur final qui appelle la racine de votre distribution renvoie l'objet racine par défaut. Par exemple, si vous désignez le fichier index.html comme objet racine par défaut, une demande pour :

```
https://d111111abcdef8.cloudfront.net/
```

Renvoie:

```
https://d111111abcdef8.cloudfront.net/index.html
```

> **Note**
>
> CloudFront ne détermine pas si une URL comportant plusieurs barres obliques de fin (`https://d111111abcdef8.cloudfront.net///`) est équivalente à. `https://d111111abcdef8.cloudfront.net/` C'est votre serveur d'origine qui effectue cette comparaison.

Si vous définissez un objet racine par défaut, une demande d'utilisateur final pour un sous-répertoire de votre distribution ne renvoie pas l'objet racine par défaut. Supposons, par exemple, qu' `index.html`il s'agisse de votre objet racine par défaut et qu'il CloudFront reçoive une demande d'utilisateur final concernant le `install` répertoire de votre CloudFront distribution :

```
https://d111111abcdef8.cloudfront.net/install/
```

CloudFront ne renvoie pas l'objet racine par défaut même si une copie de `index.html` apparaît dans le `install` répertoire. Toutefois, si vous avez spécifié un chemin vers votre objet racine par défaut, (`install/index.html`) CloudFront renverra l'objet racine par défaut pour les demandes des utilisateurs finaux concernant le répertoire `install`

Si vous configurez votre distribution pour autoriser toutes les méthodes HTTP prises en charge par CloudFront, l'objet racine par défaut s'applique à toutes les méthodes. Par exemple, si votre objet racine par défaut est index.php et que vous écrivez votre application pour envoyer une `POST` demande à la racine de votre domaine (https://example.com), CloudFront envoie la demande à https://example.com/index.php.

Le comportement des objets racine CloudFront par défaut est différent de celui des documents d'index Amazon S3. Lorsque vous configurez un compartiment Amazon S3 comme site web et que vous spécifiez le document d'index, Amazon S3 renvoie le document d'index même si un utilisateur demande un sous-répertoire du compartiment. (Une copie du document d'index doit apparaître dans chaque sous-répertoire.) Pour plus d'informations sur la configuration de compartiments Amazon S3 en tant que sites web et sur les documents d'index, consultez le chapitre Hébergement de sites web sur Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

> **Important**
>
> N'oubliez pas qu'un objet racine par défaut ne s'applique qu'à votre CloudFront distribution. Vous devez quand-même gérer la sécurité pour votre origine. Par exemple, si vous utilisez

une origine Amazon S3, vous devez tout de même définir les ACL de votre compartiment Amazon S3 de manière appropriée pour vous assurer du niveau d'accès que vous souhaitez sur votre compartiment.

Comment CloudFront fonctionne si vous ne définissez pas d'objet racine

Si vous ne définissez pas un objet racine par défaut, des demandes pour la racine de votre distribution sont transmises à votre serveur d'origine. Si vous utilisez une origine Amazon S3, l'un des éléments suivants peut être renvoyé :

- Une liste du contenu de votre compartiment Amazon S3 — Dans l'une des conditions suivantes, le contenu de votre origine est visible par tous ceux qui accèdent CloudFront à votre distribution :
  - Votre compartiment n'est pas correctement configuré.
  - Les autorisations Amazon S3 sur le compartiment associé à votre distribution et sur les objets du compartiment accordent l'accès à tout le monde.
  - Un utilisateur final accède à votre origine à l'aide de l'URL racine de votre origine.
- Une liste des contenus privés de votre origine — Si vous configurez votre origine en tant que distribution privée (vous êtes le seul à CloudFront y avoir accès), le contenu du compartiment Amazon S3 associé à votre distribution est visible par toute personne disposant des informations d'identification nécessaires pour accéder à votre distribution CloudFront. Dans ce cas, les utilisateurs ne peuvent pas accéder à vos contenus via l'URL racine de votre origine. Pour plus d'informations sur la distribution de contenus privés, consultez the section called "Restriction de contenu avec des URL et des cookies signés".
- `Error 403 Forbidden`— CloudFront renvoie cette erreur si les autorisations sur le compartiment Amazon S3 associé à votre distribution ou les autorisations sur les objets de ce compartiment interdisent l'accès à CloudFront et à tout le monde.

Invalidation de fichiers pour supprimer du contenu

Si vous devez supprimer un fichier des caches CloudFront Edge avant son expiration, vous pouvez effectuer l'une des opérations suivantes :

- Invalidez le fichier des caches périphériques. La prochaine fois qu'un utilisateur demandera le fichier, il CloudFront retournera à l'origine pour récupérer la dernière version du fichier.

- Utilisez la gestion des versions de fichiers pour offrir une version différente du fichier dont le nom diffère. Pour plus d'informations, consultez Mise à jour des fichiers existants à l'aide de noms de fichiers versionnés.

Rubriques

- Choix entre invalider des fichiers existants et utiliser des noms de fichier versionnés
- Déterminez les chemins à invalider
- Ce que vous devez savoir lorsque vous invalidez des chemins
- Invalidation de contenu par des balises de cache
- Ce que vous devez savoir lorsque vous invalidez des balises
- Invalidation de fichiers
- Paiement d'une invalidation de fichier

Choix entre invalider des fichiers existants et utiliser des noms de fichier versionnés

Pour contrôler les versions de fichiers qui sont offerts à partir de votre distribution, vous pouvez invalider des fichiers ou leur attribuer des noms de fichier versionnés. Si vous souhaitez mettre souvent vos fichiers à jour, nous vous recommandons d'utiliser principalement la gestion des versions de fichiers pour les raisons suivantes :

- La gestion des versions vous permet de contrôler quel fichier est renvoyé par une requête même lorsque l'utilisateur dispose d'une version en cache en local ou derrière un proxy de mise en cache d'entreprise. Si vous invalidez le fichier, l'utilisateur pourrait continuer de voir l'ancienne version tant qu'elle n'est pas arrivée à expiration dans ces caches.
- CloudFront les journaux d'accès incluent les noms de vos fichiers. La gestion des versions facilite donc l'analyse des résultats des modifications apportées aux fichiers.
- La gestion des versions offre un moyen d'offrir des versions différentes de fichiers à des utilisateurs différents.
- La gestion des versions simplifie la restauration par progression et la restauration entre les révisions de fichier.
- La gestion des versions est moins chère. Vous devez toujours payer pour CloudFront transférer les nouvelles versions de vos fichiers vers des emplacements périphériques, mais vous n'avez pas à payer pour l'annulation de fichiers.

Pour plus d'informations sur la gestion des versions de fichiers, consultez Mise à jour des fichiers existants à l'aide de noms de fichiers versionnés.

Déterminez les chemins à invalider

Si vous souhaitez invalider plusieurs fichiers, par exemple tous les fichiers d'un répertoire ou tous les fichiers commençant par les mêmes caractères, vous pouvez inclure le caractère générique `*` à la fin du chemin d'invalidation. Pour plus d'informations sur l'utilisation du caractère générique `*`, consultez Invalidation paths.

Pour invalider des fichiers, vous pouvez indiquer le chemin pour des fichiers individuels ou un chemin qui se termine par le caractère générique `*` qui peut s'appliquer à un ou plusieurs fichiers, comme illustré dans les exemples suivants :

- `/images/image1.jpg`
- `/images/image*`
- `/images/*`

Si vous souhaitez invalider certains fichiers mais que vos utilisateurs n'ont pas forcément à accès à chaque fichier sur votre origine, vous pouvez déterminer quels fichiers les utilisateurs ont demandés à CloudFront et n'invalider que ces fichiers. Pour déterminer les fichiers que les utilisateurs ont demandés, activez la journalisation des CloudFront accès. Pour plus d'informations sur les journaux d'accès, consultez Journaux d'accès (journaux standard).

Ce que vous devez savoir lorsque vous invalidez des chemins

Lorsque vous indiquez un fichier à invalider, consultez les informations suivantes :

Sensibilité à la casse

Les chemins d'invalidation sont sensibles à la casse. Par exemple, `/images/image.jpg` et `/images/Image.jpg` désignent deux fichiers différents.

Modification de l'URI à l'aide d'une fonction Lambda

Si votre CloudFront distribution déclenche une fonction Lambda lors d'événements de requête de l'utilisateur, et si la fonction modifie l'URI du fichier demandé, nous vous recommandons d'invalider les deux URI pour supprimer le fichier des CloudFront caches périphériques :

- L'URI de la demande utilisateur
- L'URI une fois que la fonction l'a modifié

Example Exemple

Supposons que votre fonction Lambda modifie l'URI d'un fichier, en remplaçant :

```
https://d111111abcdef8.cloudfront.net/index.html
```

par un URI qui inclut un répertoire de langue :

```
https://d111111abcdef8.cloudfront.net/en/index.html
```

Pour invalider le fichier, vous devez spécifier les chemins suivants :

- `/index.html`
- `/en/index.html`

Pour plus d'informations, consultez Invalidation paths.

Objet racine par défaut

Pour invalider l'objet racine (fichier) par défaut, spécifiez le chemin tout comme le chemin pour tout autre fichier. Pour plus d'informations, consultez Fonctionnement de l'objet racine par défaut.

Transmettre des cookies

Si vous avez configuré CloudFront pour transférer les cookies vers votre source, CloudFront les caches périphériques peuvent contenir plusieurs versions du fichier. Lorsque vous invalidez un fichier, toutes les versions mises en cache du fichier sont CloudFront invalides, quels que soient les cookies associés. Vous ne pouvez pas invalider de façon sélective certaines versions et pas d'autres en fonction des cookies associés. Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.

Transmettre des en-têtes

Si vous avez configuré CloudFront pour transmettre une liste d'en-têtes à votre origine et pour mettre en cache en fonction des valeurs des en-têtes, les caches CloudFront périphériques peuvent contenir plusieurs versions du fichier. Lorsque vous invalidez un fichier, CloudFront invalide chaque version mise en cache du fichier, quelles que soient les valeurs des en-têtes. Vous ne pouvez pas invalider de façon sélective certaines versions et pas d'autres en fonction de valeurs d'en-têtes. (Si vous configurez CloudFront pour transférer tous les en-têtes vers votre

origine, vos fichiers CloudFront ne seront pas mis en cache.) Pour plus d'informations, consultez Mise en cache de contenu basée sur des en-têtes de demandes.

Transmission de chaînes de requête

Si vous avez configuré CloudFront pour transférer les chaînes de requête vers votre origine, vous devez inclure les chaînes de requête lors de l'invalidation de fichiers, comme indiqué dans les exemples suivants :

- `/images/image.jpg?parameter1=a`
- `/images/image.jpg?parameter1=b`

Si les requêtes client incluent cinq chaînes de requête différentes pour le même fichier, vous pouvez soit invalider le fichier cinq fois (une fois par chaîne de requête), soit utiliser le caractère générique * dans le chemin d'invalidation, comme illustré dans l'exemple suivant :

```
/images/image.jpg*
```

Pour plus d'informations sur l'utilisation de caractères génériques dans le chemin d'invalidation, consultez Invalidation paths.

Pour plus d'informations sur les chaînes de requête, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête.

Pour déterminer quelles chaînes de requête sont utilisées, vous pouvez activer la journalisation des accès CloudFront. Pour plus d'informations, consultez Journaux d'accès (journaux standard).

Maximum autorisé

Pour plus d'informations sur le nombre maximum d'invalidations autorisées, consultez Quotas sur les invalidations.

Fichiers Microsoft Smooth Streaming

Vous ne pouvez pas invalider des fichiers multimédias au format Microsoft Smooth Streaming lorsque vous avez activé Smooth Streaming pour le comportement de cache correspondant.

Non-ASCII ou des caractères dangereux dans le chemin

Si le chemin inclut des caractères non ASCII ou des caractères dangereux tels que définis dans la RFC 1738, ces caractères. URL-encode N'insérez URL-encode aucun autre caractère dans le chemin, sinon cela CloudFront n'invalidera pas l'ancienne version du fichier mis à jour.

> **Important**
>
> N'utilisez pas le ~ personnage sur votre chemin. CloudFront ne prend pas en charge ce caractère pour les invalidations, que ce soit le cas URL-encoded ou non.

Chemins d'invalidation

Le chemin est relatif par rapport à la distribution. Par exemple, pour invalider le fichier à l'adresse `https://d111111abcdef8.cloudfront.net/images/image2.jpg`, vous devez spécifier `/images/image2.jpg`.

> **Note**
>
> Dans la console CloudFront, vous pouvez omettre la barre oblique de début dans le chemin, comme ci-après : `images/image2.jpg`. Lorsque vous utilisez directement l' CloudFront API, les chemins d'invalidation doivent commencer par une barre oblique.

Vous pouvez également invalider simultanément plusieurs fichiers à l'aide du caractère générique *. Le caractère générique *, qui remplace 0 caractère ou plus, doit être le dernier caractère dans le chemin d'invalidation.

> **Important**
>
> Pour utiliser des caractères génériques (*) lors de l'invalidation, vous devez placer le caractère générique à la fin du chemin. Les astérisques (*) insérés ailleurs sont traités comme une correspondance de caractères littérale au lieu d'une invalidation par un caractère générique.

Si vous utilisez le AWS Command Line Interface (AWS CLI) pour invalider des fichiers et que vous spécifiez un chemin qui inclut le * caractère générique, vous devez utiliser des guillemets (") autour du chemin, comme. `"/*"`

La longueur maximale d'un chemin est de 4 000 caractères.

Example Exemple : chemins d'invalidation

- Pour invalider tous les fichiers d'un répertoire, tous ses sous-répertoires et tous les fichiers du répertoire et des sous-répertoires :

  */ directory-path /**

- Pour invalider un répertoire, tous ses sous-répertoires, et tous les fichiers de ce répertoire et ces sous-répertoires :

  */ directory-path **

- Pour invalider tous les fichiers qui ont le même nom mais des extensions de nom de fichier différentes, comme logo.jpg, logo.png et logo.gif :

  */ directory-path / file-name .**

- Pour invalider tous les fichiers d'un répertoire dont le nom de fichier commence par les mêmes caractères (par exemple, tous les fichiers pour une vidéo au format HLS), quelle que soit l'extension du nom de fichier :

  */ directory-path / initial-characters-in-file-name **

- Lorsque vous configurez CloudFront la mise en cache en fonction des paramètres de chaîne de requête et que vous souhaitez invalider chaque version d'un fichier :

  */ directory-path / file-name . file-name-extension **

- Pour invalider tous les fichiers dans une distribution :

  /*

Pour plus d'informations sur l'invalidation de fichiers si vous utilisez une fonction Lambda pour modifier l'URI, consultez Changing the URI Using a Lambda Function.

Si le chemin d'invalidation est un répertoire et que vous n'avez pas adopté une méthode standardisée pour spécifier les répertoires, avec ou sans barre oblique de fin (/), nous vous recommandons d'invalider le répertoire avec et sans barre oblique de fin, par exemple, `/images` et `/images/`.

URL signées

Si vous utilisez des URL signées, invalidez un fichier en n'incluant que la portion de l'URL avant le point d'interrogation (?).

Invalidation de contenu par des balises de cache

Amazon CloudFront prend en charge les invalidations de balises, ce qui vous permet d'invalider les objets mis en cache en fonction de balises sémantiques plutôt que de chemins d'URL. Cela vous permet de contrôler de manière flexible l'invalidation du cache sans que votre structure d'URL corresponde à votre stratégie d'invalidation.

Avant d'invalider du contenu à l'aide de balises de cache, passez en revue les exigences et les points à prendre en compte dansCe que vous devez savoir lorsque vous invalidez des balises.

Comment fonctionne l'invalidation des balises

1. Configurez votre distribution : ajoutez un `CacheTagConfig` à votre distribution en spécifiant le nom d'en-tête HTTP que votre origine utilise pour renvoyer les balises de cache.
2. Marquez les objets à votre origine : lorsque vous renvoyez un objet que vous souhaitez mettre en cache avec des balises, configurez votre origine pour inclure l'en-tête spécifié dans les réponses HTTP avec des valeurs de balises séparées par des virgules.

```
HTTP/1.1 200 OK
Content-Type: text/html
x-amz-meta-cache-tag: product:electronics, category:tv, brand:example
Cache-Control: max-age=3600
```

> **Note**
>
> Pour les origines S3, vous pouvez joindre des balises de cache à vos objets S3 en tant que métadonnées. Vous pouvez ajouter une entrée de métadonnées avec la clé de votre choix (exemple : `cache-tag`) et une liste de balises séparées par des virgules comme valeur (exemple :`product:electronics, category:tv, brand:example`). S3 affiche les métadonnées des objets sous forme d'en-têtes de réponse préfixés par `x-amz-meta-<Key>`, de sorte qu'une clé de métadonnées de `cache-tag` serait renvoyée sous forme d'`x-amz-meta-cache-tag`en-tête. Vous pouvez le configurer `HeaderName` dans votre `CacheTagConfig` `x-amz-meta-cache-tag` to pour activer l'envoi d'invalidations à ces balises.

> **Note**
>
> Vous pouvez également associer une fonction Lambda @Edge de réponse d'origine à votre comportement de cache pour ajouter des en-têtes de balises de cache. Si vous utilisez Lambda @Edge, le nom de l'en-tête n'a pas besoin de suivre le `x-amz-meta-<Key>` format.

3. Invalider par balise : utilisez l' `CreateInvalidation`API avec le # préfixe pour invalider tous les objets mis en cache avec la balise spécifiée.

```
aws cloudfront create-invalidation \
  --distribution-id distribution_ID \
  --paths "#product:electronics"
```

Cela invalide TOUS les objets mis en cache qui contiennent la balise `product:electronics`, quel que soit leur chemin d'URL.

Exigences relatives au format des balises

Valeur de l'en-tête de réponse d'origine :

- Les balises sont séparées par des virgules dans la valeur de l'en-tête.
- Les espaces de début et de fin autour de chaque étiquette sont supprimés.
- Les deux `tag1,tag2,tag3` `tag1, tag2, tag3` sont valides et équivalents.

Valeurs des balises individuelles :

- Caractères ASCII visibles (33—126)
- Pas de caractères de contrôle, d'espaces ou de virgules
- Case-insensitive
- 256 caractères maximum par tag
- Maximum de 50 balises par objet (les balises supplémentaires sont ignorées)

Configuration d'une distribution pour les invalidations de balises

Pour activer les invalidations de balises, ajoutez a `CacheTagConfig` à votre configuration de distribution :

```
aws cloudfront create-distribution \
  --distribution-config '{
    "CallerReference": "my-distribution",
    "CacheTagConfig": {
      "HeaderName": "x-amz-meta-cache-tag"
    },
    "DefaultCacheBehavior": {
      "TargetOriginId": "myOrigin",
      "ViewerProtocolPolicy": "redirect-to-https",
      "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e58f6"
    },
    "Origins": { ... },
    "Enabled": true,
    "Comment": "Distribution with tag support"
  }'
```

Création d'invalidations de balises

Utilisez le # préfixe du `--paths` paramètre pour spécifier les balises :

```
# Invalidate all objects tagged with "user1"
aws cloudfront create-invalidation \
  --distribution-id distribution_ID \
  --paths "#user1"

# Invalidate objects matching any of multiple tags (OR logic)
aws cloudfront create-invalidation \
  --distribution-id distribution_ID \
  --paths "#user1" "#product-category:electronics"

# Mix path and tag invalidations in one batch
aws cloudfront create-invalidation \
  --distribution-id distribution_ID \
  --paths "/index.html" "#user1" "/images/*" "#product-category:electronics"
```

Vérification de l'état d'invalidation

`GetInvalidation`Utilisez-le pour vérifier l'état. La réponse inclut à la fois des éléments de chemin et de balise :

```
aws cloudfront get-invalidation \
  --distribution-id distribution_ID \
  --id invalidation_ID
```

Considérations importantes

- Opt-in obligatoire : l'invalidation des balises ne fonctionne que sur les distributions qui ont été `CacheTagConfig` configurées. Les distributions sans cette configuration ignorent les en-têtes de balises de cache depuis l'origine.
- Limites de traitement des balises : CloudFront traite jusqu'à 50 balises par objet mis en cache. Si une réponse d'origine contient plus de 50 balises, les balises supplémentaires au-delà de la limite ne sont pas stockées.
- Modification du nom de l'en-tête : les invalidations de balises sont comparées à la configuration actuelle`CacheTagConfig`. Si vous modifiez ce paramètre`CacheTagConfig`, `HeaderName` les invalidations émises pour les objets mis en cache avec des balises sous l'ancien nom d'en-tête ne seront plus évaluées. Si vous devez modifier le nom de l'en-tête, commencez à renvoyer les nouveaux et les anciens en-têtes des balises de cache avec vos objets, puis annulez le chemin (par exemple`/*`) ou invalidez les balises existantes avant de modifier le nom de l'en-tête pour éviter de diffuser du contenu obsolète. Une fois cela fait, vous pouvez arrêter d'envoyer l'ancien en-tête des balises de cache avec vos objets.
- Suppression CacheTagConfig : lorsque vous supprimez `CacheTagConfig` d'une distribution, CloudFront arrête d'extraire les balises des réponses d'origine. Les objets mis en cache existants avec des balises sont servis normalement jusqu'à leur expiration ou leur invalidation par path.
- Compatibilité descendante : les invalidations de chemin et de caractères génériques existantes continuent de fonctionner sans modification. Les invalidations de balises s'additionnent : vous pouvez utiliser les deux méthodes sur la même distribution.
- Locataires de distribution : l'invalidation des balises est également prise en charge pour les locataires de distribution à l'aide de l'`CreateInvalidationForDistributionTenant`API.

Exemples de cas d’utilisation

Exemple 1 : catalogue E-commerce de produits

Un site de commerce électronique étiquette les pages de produits mises en cache avec le produit, la catégorie et la marque :

```
x-amz-meta-cache-tag: category:electronics, brand:acme, product:12345
```

Lorsque ACME met à jour sa marque, invalidez tous les produits ACME en une seule fois :

```
aws cloudfront create-invalidation \
  --distribution-id distribution_ID \
  --paths "#brand:acme"
```

Exemple 2 : plateforme User-generated de contenu

Une plateforme étiquette le contenu mis en cache à l'aide de l'identifiant utilisateur du propriétaire :

```
x-amz-meta-cache-tag: user:12345, content-type:image
```

Lorsqu'un utilisateur ferme son compte, invalidez tout son contenu une fois que vous l'avez supprimé de l'origine :

```
aws cloudfront create-invalidation \
  --distribution-id distribution_ID \
  --paths "#user:12345"
```

Exemple 3 : Versionnage du contenu

Un CMS étiquette le contenu à l'aide d'identifiants de version :

```
x-amz-meta-cache-tag: version:v2, template:homepage
```

Lors du déploiement d'une nouvelle version, invalidez tout le contenu de la v2 :

```
aws cloudfront create-invalidation \
  --distribution-id distribution_ID \
  --paths "#version:v2"
```

Ce que vous devez savoir lorsque vous invalidez des balises

Lorsque vous spécifiez une balise à invalider, reportez-vous aux informations suivantes :

Opt-in requis

L'invalidation des balises ne fonctionne que sur les distributions qui ont été `CacheTagConfig` configurées. Les distributions sans cette configuration ignorent les en-têtes de balises de cache depuis l'origine. Pour plus d'informations, consultez Invalidation de contenu par des balises de cache.

Préfixe d'invalidation des balises

Les éléments d'invalidation des balises doivent commencer par le # personnage. Par exemple, pour invalider tous les objets mis en cache marqués avec`product:electronics`, spécifiez-les `#product:electronics` dans la `Paths.Items` liste.

Sensibilité à la casse

Les valeurs des balises ne distinguent pas les majuscules et minuscules. Par exemple, `#Product:Electronics` et `#product:electronics` faites référence à la même étiquette.

Format de balise

Chaque valeur de balise doit contenir uniquement des caractères ASCII visibles (33 à 126), à l'exception des virgules. La longueur maximale d'une balise est de 256 caractères.

Pas de support pour les caractères génériques

Contrairement aux invalidations de chemin, les éléments d'invalidation des balises ne prennent pas en charge le caractère générique. * Chaque élément # préfixé correspond à la valeur exacte de la balise.

Nombre maximum de balises par objet mis en cache

CloudFront traite jusqu'à 50 balises par objet mis en cache. Si une réponse d'origine contient plus de 50 balises dans l'en-tête configuré, les balises supplémentaires au-delà de la limite ne sont pas stockées et ne peuvent pas être utilisées pour l'invalidation.

Transfert de cookies, d'en-têtes et de chaînes de requête

Lorsque vous invalidez par balise, CloudFront invalide chaque variante mise en cache de chaque objet qui porte la balise spécifiée, quels que soient les cookies, les en-têtes ou les paramètres de chaîne de requête associés. Vous ne pouvez pas invalider certaines variantes de manière sélective et pas d'autres.

Invalidations mixtes de chemins et de balises

Vous pouvez inclure à la fois des éléments de chemin (par exemple`/images/*`) et des éléments de balise (par exemple`#brand:acme`) dans le même lot d'invalidation d'une `CreateInvalidation` demande. Chaque élément compte comme un chemin d'invalidation vers vos limites.

Maximum autorisé

Les éléments d'invalidation des balises sont pris en compte dans les mêmes limites d'invalidation simultanées que les éléments du chemin. Chaque élément de balise compte comme un chemin d'invalidation. Pour plus d’informations, consultez Quotas sur les invalidations.

Changer le nom de l'en-tête

Si vous modifiez l'entrée`CacheTagConfig`, `HeaderName` les invalidations émises pour les balises extraites sous l'ancien nom d'en-tête ne seront plus évaluées. Avant de modifier le nom de l'en-tête :

1. Commencez à renvoyer les anciens et les nouveaux en-têtes de balises de cache depuis votre origine.
2. Invalidez un chemin (par exemple`/*`) ou invalidez les balises existantes.
3. Mettez à jour `CacheTagConfig` avec le nouveau`HeaderName`.
4. Arrêtez de renvoyer l'ancien en-tête depuis votre origine.

Locataires de distribution

L'invalidation des balises est également prise en charge pour les locataires de distribution à l'aide de l' `CreateInvalidationForDistributionTenant`API.

Invalidation de fichiers

Vous pouvez utiliser la CloudFront console pour créer et exécuter une invalidation, afficher la liste des invalidations que vous avez soumises précédemment et afficher des informations détaillées sur une invalidation individuelle. Vous pouvez également copier une invalidation existante, modifier la liste des chemins de fichier et exécuter l’invalidation modifiée. Vous ne pouvez pas supprimer d’invalidations de la liste.

Table des matières

- Invalidation de fichiers

- Copie, modification et réexécution d’une invalidation existante
- Annulation des invalidations
- Liste des invalidations
- Affichage des informations sur une invalidation

Invalidation de fichiers

Pour invalider des fichiers à l'aide de la CloudFront console, procédez comme suit.

Console

Pour invalider des fichiers (console)

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution pour laquelle vous voulez invalider des fichiers.
3. Choisissez l’onglet Invalidations.
4. Sélectionnez Créer une invalidation.
5. Pour les fichiers que vous voulez invalider, entrez un chemin d’invalidation par ligne. Pour plus d’informations sur la spécification de chemins d’invalidation, consultez Ce que vous devez savoir lorsque vous invalidez des chemins.

   > **Important**
   >
   > Indiquez les chemins de fichier avec soin. Vous ne pouvez pas annuler une demande d’invalidation après l’avoir commencée.

6. Sélectionnez Créer une invalidation.

CloudFront API

Pour en savoir plus sur l'invalidation d'objets et l'affichage d'informations sur les invalidations, consultez les rubriques suivantes dans le manuel Amazon API Reference : CloudFront

- CreateInvalidation
- ListInvalidations
- GetInvalidation

> **Note**
>
> Si vous utilisez le AWS Command Line Interface (AWS CLI) pour invalider des fichiers et que vous spécifiez un chemin qui inclut le * caractère générique, vous devez placer le chemin entre guillemets ("), comme dans l'exemple suivant :
>
> ```
> aws cloudfront create-invalidation --distribution-id distribution_ID --paths
>  "/*"
> ```

Copie, modification et réexécution d'une invalidation existante

Vous pouvez copier une invalidation que vous avez créée précédemment, mettre à jour la liste des chemins d'invalidation d'objet et exécuter l'invalidation mise à jour. Vous ne pouvez pas copier une invalidation existante, mettre à jour la liste des chemins d'invalidation, puis enregistrer l'invalidation mise à jour sans l'exécuter.

> **Important**
>
> Si vous copiez une invalidation toujours en cours, mettez à jour la liste des chemins d'invalidation, puis exécutez l'invalidation mise à jour, cela n'arrêtera ni CloudFront ne supprimera l'invalidation que vous avez copiée. Si des chemins d'invalidation apparaissent dans l'original et dans la copie, CloudFront vous tenterez d'invalider les fichiers deux fois, et les deux invalidations seront prises en compte dans votre nombre maximum d'invalidations gratuites pour le mois. Si vous avez déjà atteint le nombre maximal d'invalidations gratuites, les deux invalidations vous seront facturées pour chaque fichier. Pour plus d'informations, consultez Quotas sur les invalidations.

Pour copier, modifier et réexécuter une invalidation existante

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution qui contient l'invalidation à copier.
3. Choisissez l'onglet Invalidations.
4. Sélectionnez l'invalidation que vous souhaitez copier.

Si vous n'êtes pas sûr de l'invalidation à copier, vous pouvez choisir une invalidation et sélectionner Afficher les détails pour afficher des informations détaillées sur cette invalidation.

5. Choisissez Copier vers un nouvel élément.
6. Mettez à jour la liste des chemins d'invalidation la cas échéant.
7. Sélectionnez Créer une invalidation.

Annulation des invalidations

Lorsque vous soumettez une demande d'invalidation à CloudFront, la CloudFront transmet à tous les emplacements périphériques en quelques secondes, et chaque emplacement périphérique commence immédiatement à traiter l'invalidation. De ce fait, vous ne pouvez pas annuler une invalidation après l'avoir soumise.

Liste des invalidations

Vous pouvez afficher la liste des 100 dernières invalidations que vous avez créées et exécutées pour une distribution à l'aide de la CloudFront console. Si vous souhaitez obtenir une liste de plus de 100 invalidations, utilisez l'opération d'API `ListInvalidations`. Pour plus d'informations, consultez ListInvalidations le manuel Amazon CloudFront API Reference.

Pour répertorier des invalidations

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution pour laquelle vous voulez afficher une liste d'invalidations.
3. Choisissez l'onglet Invalidations.

> **Note**
>
> Vous ne pouvez pas supprimer d'invalidations de la liste.

Affichage des informations sur une invalidation

Vous pouvez afficher des informations détaillées sur une invalidation, notamment l'ID de distribution, l'ID d'invalidation, le statut de l'invalidation, la date et l'heure auxquelles l'invalidation a été créée, et une liste complète des chemins d'invalidation.

Pour afficher des informations sur une invalidation

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution qui contient l'invalidation pour laquelle vous souhaitez afficher des informations détaillées.
3. Choisissez l'onglet Invalidations.
4. Choisissez l'ID d'invalidation applicable ou sélectionnez l'ID d'invalidation, puis sélectionnez Afficher les détails.

Paiement d'une invalidation de fichier

Les premiers 1 000 chemins d'invalidation que vous soumettez par mois sont gratuits ; vous paierez pour chaque chemin d'invalidation au-delà de 1 000 au cours d'un mois. Un chemin d'invalidation peut être un fichier unique (comme `/images/logo.jpg`) ou plusieurs fichiers (comme `/images/*`). Un chemin qui inclut le `*` caractère générique est considéré comme un seul chemin même s'il entraîne CloudFront l'invalidation de milliers de fichiers.

Le maximum de 1 000 chemins d'invalidation gratuits par mois s'applique au nombre total de chemins d'invalidation pour toutes les distributions que vous créez avec un Compte AWS. Par exemple, supposons que vous utilisiez le Compte AWS `john@example.com` pour créer trois distributions et que vous soumettiez 600 chemins d'invalidation pour chaque distribution au cours d'un mois donné (pour un total de 1 800 chemins d'invalidation). Dans ce cas, la différence entre le nombre total de chemins d'invalidation et la limite de 1 000 entrées gratuites vous AWS sera facturée. Dans cet exemple, nous vous AWS facturerons 800 chemins d'invalidation au cours de ce mois-là.

Les frais pour soumettre un chemin d'invalidation sont les mêmes quel que soit le nombre de fichiers que vous invalidez : un seul fichier (`/images/logo.jpg`) ou tous les fichiers associés à une distribution (`/*`). Étant donné que la facturation est appliquée par chemin dans une demande d'invalidation, regrouper plusieurs chemins dans une même demande ne change rien : chaque chemin est comptabilisé individuellement pour la facturation.

Pour plus d'informations sur la tarification d'invalidation, consultez la page CloudFront Tarification https://aws.amazon.com/cloudfront/pricing/ Amazon. Pour plus d'informations sur les chemins d'invalidation, consultez Invalidation paths.

Les chemins d'invalidation des balises sont pris en compte dans le même quota de 1 000 chemins d'invalidation gratuits par mois. Par exemple, si vous soumettez 500 invalidations de chemin et 600 invalidations de balises par mois (pour un total de 1 100 chemins d'invalidation), 100 chemins d'invalidation vous sont facturés. Un élément d'invalidation de balise unique (par exemple `#product:electronics`) est considéré comme un chemin quel que soit le nombre d'objets mis en cache qu'il invalide. Tout comme l'invalidation d'un chemin par un caractère générique (par exemple, `/*`) compte comme un seul chemin.

Pour plus d'informations sur l'invalidation des balises, consultezInvalidation de contenu par des balises de cache.

Diffusion de fichiers compressés

Lorsque les objets demandés sont compressés, les téléchargements peuvent être plus rapides, parce que les objets sont plus petits (dans certains cas, inférieurs à un quart de la taille de l'objet original). Des téléchargements plus rapides peuvent accélérer le rendu des pages Web pour vos utilisateurs, en particulier pour JavaScript les fichiers CSS. En outre, le coût du transfert de CloudFront données est basé sur la quantité totale de données diffusées. La diffusion d'objets compressés peut être moins coûteux que la diffusion d'objets non compressés.

Rubriques

- Configurer CloudFront pour compresser des objets
- Comment fonctionne CloudFront la compression
- Conditions de compression
- Types de fichiers qui CloudFront compressent
- Conversion de l'en-tête ETag

Configurer CloudFront pour compresser des objets

CloudFront Pour configurer la compression des objets, mettez à jour le comportement du cache que vous souhaitez utiliser pour les objets compressés.

Pour configurer CloudFront la compression d'objets (console)

1. Connectez-vous à la console CloudFront.
2. Choisissez votre distribution, puis le Comportement à modifier.
3. Pour le paramètre Compresser automatiquement les objets, choisissez Oui.
4. Utilisez une politique de cache pour spécifier les paramètres de mise en cache et activez les formats de compression Gzip et Brotli.

> **Remarques**
>
> - Vous devez utiliser des politiques de cache pour utiliser la compression Brotli. Brotli ne prend pas en charge les anciens paramètres de cache.
> - Pour activer la compression à l'aide de l'CloudFrontAPI CloudFormationou de l'APICompress, définissez `EnableAcceptEncodingBrotli` les paramètres`EnableAcceptEncodingGzip`, sur`true`.

Pour comprendre comment CloudFront compresse les objets, reportez-vous à la section suivante.

Comment fonctionne CloudFront la compression

1. Un utilisateur demande un objet. L'utilisateur inclut l'en-tête HTTP `Accept-Encoding` dans la demande et les valeurs d'en-tête incluent `gzip`, `br` ou les deux. Cela signifie qu'il prend en charge les objets compressés. Lorsque le visualiseur supporte à la fois Gzip et Brotli, CloudFront il utilise Brotli.

   > **Note**
   >
   > Les navigateurs web Chrome et Firefox prennent en charge la compression Brotli uniquement lorsque la demande est envoyée en HTTPS. Ils ne prennent pas en charge Brotli avec les demandes HTTP.

2. À l'emplacement périphérique, CloudFront recherche dans le cache une copie compressée de l'objet demandé.
3. Selon que l'objet compressé se trouve dans le cache ou non, CloudFront effectue l'une des opérations suivantes :

- Si l'objet compressé est déjà dans le cache, CloudFront envoie l'objet au visualiseur et ignore les étapes restantes.
- Si l'objet compressé ne se trouve pas dans le cache, CloudFront transmet la demande à l'origine.

> **Note**
>
> Si une copie non compressée de l'objet se trouve déjà dans le cache, vous CloudFront pouvez l'envoyer au visualiseur sans transmettre la demande à l'origine. Par exemple, cela peut se produire lorsque la compression a CloudFront été précédemment ignorée. Dans ce cas, met en CloudFront cache l'objet non compressé et continue de le servir jusqu'à ce que l'objet expire, soit expulsé ou soit invalidé.

4. Si l'origine renvoie un objet compressé (comme indiqué par l'`Content-Encoding`en-tête de la réponse HTTP), CloudFront envoie l'objet compressé au visualiseur, l'ajoute au cache et ignore les étapes restantes. CloudFront ne compresse pas à nouveau l'objet.
5. Si l'origine renvoie un objet non compressé CloudFront sans l'`Content-Encoding`en-tête dans la réponse HTTP, CloudFront elle détermine si l'objet peut être compressé. Pour de plus amples informations, veuillez consulter Conditions de compression.
6. Si l'objet peut être compressé CloudFront , compressez-le, envoyez-le au visualiseur, puis ajoutez-le au cache.
7. S'il y a des demandes ultérieures du spectateur pour le même objet, CloudFront renvoie la première version mise en cache. Par exemple, si un utilisateur demande un objet spécifique mis en cache utilisant la compression Gzip et que l'utilisateur accepte le format Gzip, les demandes ultérieures pour ce même objet renverront toujours la version Gzip, même si l'utilisateur accepte à la fois Brotli et Gzip.

Certaines origines personnalisées peuvent également compresser des objets. Votre origine est peut-être en mesure de compresser des objets qui CloudFront ne le sont pas. Pour de plus amples informations, veuillez consulter Types de fichiers qui CloudFront compressent.

Conditions de compression

La liste suivante fournit plus d'informations sur les scénarios dans lesquels les objets CloudFront ne sont pas compressés.

La demande utilise HTTP 1.0

Si une demande CloudFront utilise le protocole HTTP 1.0, CloudFront supprime l'`Accept-Encoding`en-tête et ne compresse pas l'objet dans la réponse.

En-tête de demande **`Accept-Encoding`**

Si l'`Accept-Encoding`en-tête est absent de la demande du visualiseur, ou s'il ne contient pas `gzip` ou `br` ne contient pas de valeur, l'objet CloudFront n'est pas compressé dans la réponse. Si l'`Accept-Encoding`en-tête inclut des valeurs supplémentaires telles que`deflate`, les CloudFront supprime avant de transmettre la demande à l'origine.

Lorsqu'il CloudFront est configuré pour compresser des objets, il inclut automatiquement l'`Accept-Encoding`en-tête dans la clé de cache et dans les demandes d'origine.

Le contenu est déjà mis en cache lorsque vous configurez CloudFront pour compresser des objets

CloudFront compresse les objets lorsqu'il les extrait de l'origine. Lorsque vous configurez CloudFront pour compresser des objets, CloudFront cela ne compresse pas les objets déjà mis en cache dans des emplacements périphériques. En outre, lorsqu'un objet mis en cache expire dans un emplacement périphérique et CloudFront transmet une autre demande pour l'objet à votre origine, CloudFront cela ne compresse pas l'objet lorsque votre origine renvoie un code d'état HTTP 304. Cela signifie que l'emplacement périphérique dispose déjà de la dernière version de l'objet. Si vous souhaitez CloudFront compresser des objets déjà mis en cache dans des emplacements périphériques, vous devez invalider ces objets. Pour de plus amples informations, veuillez consulter Invalidation de fichiers pour supprimer du contenu.

L'origine est déjà configurée pour compresser les objets

Si vous configurez CloudFront pour compresser des objets et que l'origine compresse également des objets, l'origine doit inclure un `Content-Encoding` en-tête. Cet en-tête indique CloudFront que l'objet est déjà compressé. Lorsqu'une réponse provenant d'une origine inclut l'`Content-Encoding`en-tête, CloudFront elle ne compresse pas l'objet, quelle que soit la valeur de l'en-tête. CloudFrontenvoie la réponse au spectateur et met en cache l'objet à l'emplacement périphérique.

Types de fichiers qui CloudFront compressent

Pour obtenir la liste complète, consultez Types de fichiers qui CloudFront compressent.

Taille des objets qui CloudFront compressent

CloudFront compresse les objets dont la taille est comprise entre 1 000 et 10 000 000 octets.

En-tête **`Content-Length`**

L'origine doit inclure un `Content-Length` en-tête dans la réponse, qui CloudFront permet de déterminer si la taille de l'objet se situe dans la plage de CloudFront compression. Si l'`Content-Length`en-tête est absent, contient une valeur non valide ou contient une valeur en dehors de la plage de tailles qui CloudFront compresse, CloudFront cela ne compresse pas l'objet. Pour plus d'informations sur le CloudFront traitement des objets de grande taille pouvant dépasser la plage de tailles, consultezComment CloudFront traite les demandes partielles pour un objet (range GETs).

Code d'état HTTP de la réponse

CloudFront compresse les objets uniquement lorsque le code d'état HTTP de la réponse est `200`403, ou`404`.

La réponse n'a pas de corps

Lorsque la réponse HTTP de l'origine n'a pas de corps, il n'y a rien CloudFront à compresser.

En-tête **`ETag`**

CloudFront modifie parfois l'`ETag`en-tête de la réponse HTTP lorsqu'elle compresse des objets. Pour de plus amples informations, veuillez consulter the section called “Conversion de l'en-tête ETag”.

CloudFront ignore la compression

CloudFront compresse les objets au mieux. Dans de rares cas, CloudFront ignore la compression d'un objet en cas de CloudFront forte charge de trafic. CloudFront prend cette décision en fonction de divers facteurs, y compris la capacité de l'hôte. Si la compression CloudFront d'un objet est ignorée, il met en cache l'objet non compressé et continue de le servir aux utilisateurs jusqu'à ce que l'objet expire, soit expulsé ou soit invalidé.

Types de fichiers qui CloudFront compressent

Si vous configurez CloudFront pour compresser des objets, compresse CloudFront uniquement les objets dont l'en-tête de `Content-Type` réponse contient l'une des valeurs suivantes :

- `application/dash+xml`
- `application/eot`
- `application/font`

- application/font-sfnt
- application/javascript
- application/json
- application/opentype
- application/otf
- application/pdf
- application/pkcs7-mime
- application/protobuf
- application/rss+xml
- application/truetype
- application/ttf
- application/vnd.apple.mpegurl
- application/vnd.mapbox-vector-tile
- application/vnd.ms-fontobject
- application/wasm
- application/xhtml+xml
- application/xml
- application/x-font-opentype
- application/x-font-truetype
- application/x-font-ttf
- application/x-httpd-cgi
- application/x-javascript
- application/x-mpegurl
- application/x-opentype
- application/x-otf
- application/x-perl
- application/x-ttf
- font/eot
- font/opentype
- font/otf

- font/ttf
- image/svg+xml
- text/css
- text/csv
- text/html
- text/javascript
- text/js
- text/plain
- text/richtext
- text/tab-separated-values
- text/xml
- text/x-component
- text/x-java-source
- text/x-script
- vnd.apple.mpegurl

Conversion de l'en-tête **ETag**

Lorsque l'objet décompressé depuis l'origine inclut un en-tête ETag HTTP valide et fort, et qu'il CloudFront compresse l'objet, convertit CloudFront également la valeur d'ETagen-tête forte en valeur faible ETag et renvoie la ETag valeur faible au visualiseur. Les utilisateurs peuvent stocker la valeur ETag faible et l'utiliser pour envoyer des demandes conditionnelles avec l'en-tête HTTP If-None-Match. Cela permet aux utilisateurs et à l'origine de traiter les versions compressées et non compressées d'un objet comme sémantiquement équivalentes, ce qui réduit les transferts de données inutiles. CloudFront

Une valeur d'en-tête ETag valide et forte commence et se termine par des guillemets doubles (''). Pour convertir la valeur ETag forte en valeur faible, CloudFront ajoute les caractères W/ au début de la valeur ETag forte.

Lorsque l'objet de l'origine inclut une faible valeur d'ETagen-tête (une valeur qui commence par les caractèresW/), CloudFront ne modifie pas cette valeur et la renvoie au visualiseur telle qu'elle a été reçue de l'origine.

Lorsque l'objet de l'origine inclut une valeur d'`ETag`en-tête non valide (la valeur ne commence pas par '' ou par`W/`), CloudFront supprime l'`ETag`en-tête et renvoie l'objet au visualiseur sans l'en-tête de `ETag` réponse.

Pour plus d’informations, consultez les pages suivantes dans les documents web MDN :

- Directives (en-tête HTTP `ETag`)
- Validation faible (requêtes conditionnelles HTTP)
- En-tête HTTP If-None-Match

Utilisation AWS WAF protections

Vous pouvez l'utiliser AWS WAF pour protéger vos CloudFront distributions et vos serveurs d'origine. AWS WAF est un pare-feu d'applications Web qui permet de sécuriser vos applications Web et vos API en bloquant les requêtes avant qu'elles n'atteignent vos serveurs. Pour plus d'informations, consultez Accélérez et protégez vos sites Web à l'aide de CloudFront et AWS WAF et Directives de mise en œuvre AWS WAF.

Pour activer AWS WAF les protections, vous pouvez :

- Utilisez une protection à choix unique dans la CloudFront console. One-choose protection crée une liste de contrôle d'accès AWS WAF Web (ACL Web), configure des règles pour protéger vos serveurs contre les menaces Web courantes et associe l'ACL Web à la CloudFront distribution pour vous. Les rubriques de cette section supposent l'utilisation de protections à choix unique.
- Utilisez une ACL Web (liste de contrôle d'accès) préconfigurée que vous créez dans la AWS WAF console ou à l'aide AWS WAF des API. Pour plus d'informations, consultez les listes de contrôle d'accès Web (ACL) dans le Guide du AWS WAF développeur et les AssociateWeb ACL dans la référence des AWS WAF API

Vous pouvez l'activer AWS WAF lorsque vous :

- Créer une distribution
- Utilisation du tableau de bord Sécurité pour modifier les paramètres de sécurité d'une distribution existante

Lorsque vous utilisez une protection à choix unique, CloudFront applique un ensemble de protections AWS recommandé qui :

- Bloquer les adresses IP contre les menaces potentielles en vous basant sur les informations internes d'Amazon sur les menaces.
- Vous protéger contre les vulnérabilités les plus courantes détectées dans les applications Web, comme décrit dans le Top 10 de l'OWASP.
- Vous défendre contre les acteurs malveillants qui découvrent des vulnérabilités dans les applications.

> **Important**
>
> Vous devez l'activer AWS WAF si vous souhaitez afficher les mesures de sécurité dans le tableau de bord CloudFront de sécurité. Si cette option n'est pas activée AWS WAF, vous ne pouvez utiliser le tableau de bord Sécurité que pour activer AWS WAF ou configurer les restrictions CloudFront géographiques. Pour plus d'informations sur le tableau de bord, consultez Gérer AWS WAF protections de sécurité dans le tableau de bord CloudFront de sécurité plus loin dans cette section.

Rubriques

- Enable AWS WAF pour les distributions
- Gérer AWS WAF protections de sécurité dans le tableau de bord CloudFront de sécurité
- Configuration de la limitation du débit
- Désactiver AWS WAF protections de sécurité

Enable AWS WAF pour les distributions

Vous pouvez l'activer AWS WAF lorsque vous créez une distribution, ou vous pouvez activer les protections de sécurité pour une liste de contrôle d'accès (ACL) existante.

Si vous l'activez AWS WAF pour votre CloudFront distribution, vous pouvez également activer le contrôle des robots et configurer la protection de sécurité par catégorie de robots.

Rubriques

- Enable AWS WAF pour une nouvelle distribution
- Utilisation d'une ACL Web existante
- Activation du contrôle des bots
- Configuration de la protection par catégorie de bot

Enable AWS WAF pour une nouvelle distribution

La procédure suivante explique comment l'activer AWS WAF lorsque vous créez une nouvelle CloudFront distribution.

Pour activer AWS WAF pour une nouvelle distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez Créer une distribution.
3. Au besoin, suivez les étapes décrites dans Créer une distribution.
4. Dans la section Pare-feu d'application web, choisissez Modifier, puis Activer les protections de sécurité.
5. Renseignez les champs suivants :

   - Utiliser le mode de surveillance : vous pouvez activer le mode de surveillance si vous souhaitez d'abord collecter des données afin de tester la protection. Lorsque vous activez le mode de surveillance, les demandes ne sont pas bloquées si les protections étaient actives. À la place, le mode de surveillance collecte des données sur les demandes qui seraient bloquées si les protections étaient actives. Lorsque vous êtes prêt à commencer le blocage, vous pouvez l'activer sur la page Sécurité.
   - Protections supplémentaires : choisissez les options que vous souhaitez activer. Si vous activez la limitation de débit, consultez the section called "Configuration de la limitation du débit" pour plus d'informations.
   - Estimation de prix — Vous pouvez ouvrir la section pour afficher un champ dans lequel vous entrez un numéro différent requests/month et vous verrez une nouvelle estimation.
6. Vérifiez les autres paramètres de distribution, puis choisissez Créer une distribution.

Après avoir créé une distribution, CloudFront crée un tableau de bord de sécurité. Vous pouvez utiliser ce tableau de bord pour activer ou désactiver AWS WAF. Si vous ne l'avez pas AWS WAF encore activé, les tableaux et graphiques du tableau de bord restent vides.

Utilisation d'une ACL Web existante

Si vous possédez déjà une ACL Web, vous pouvez l'utiliser à la place de la protection offerte par AWS WAF.

Pour utiliser un AWS WAF configuration

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Effectuez l'une des actions suivantes :

a. Choisissez Créer une distribution et suivez les étapes indiquées dans Créer une distribution, puis revenez à cette rubrique.

b. Choisissez une configuration existante, puis sélectionnez l'onglet Sécurité.

3. Dans la section Pare-feu d'application web (WAF), sélectionnez Modifier, puis Activer les protections de sécurité.
4. Choisissez Utiliser la configuration WAF existante. Cette option apparaît uniquement si des ACL Web sont configurées.
5. Choisissez votre ACL Web existante dans le tableau Choisir une ACL Web.
6. Vérifiez les autres paramètres de distribution, puis choisissez Créer une distribution.

Activation du contrôle des bots

Si vous activez AWS WAF votre CloudFront distribution, vous pouvez consulter les demandes des robots pour une période donnée dans le tableau de bord de sécurité de la CloudFront console. Vous pouvez également activer ou désactiver le contrôle des bots ici.

Vous encourez des frais lorsque vous activez le contrôle des bots. Le tableau de bord de sécurité fournit une estimation des coûts.

Si vous activez le contrôle des bots, le tableau de bord de sécurité affiche le trafic des bots par type et catégorie de bot. Si vous désactivez le contrôle des bots, le trafic des bots est affiché en fonction de l'échantillonnage des demandes.

Pour activer le contrôle des bots

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez modifier.
3. Choisissez l'onglet Security (Sécurité).
4. Faites défiler la page jusqu'à la section Demandes de bots pour une plage de temps donnée et choisissez Activer le contrôle des bots.
5. Dans la boîte de dialogue Contrôle des bots, sous Configuration, cochez la case Activer le contrôle des bots pour les bots courants.
6. Cliquez sur Enregistrer les modifications.

Configuration de la protection par catégorie de bot

Lorsque vous activez le contrôle des bots, vous avez la possibilité de configurer la façon dont chaque bot non vérifié est traité par catégorie de bot. Par exemple, vous pouvez configurer un bot de bibliothèque HTTP sur le Mode Surveillance et attribuer un Défi à un vérificateur de lien.

> **Note**
>
> Les robots connus AWS pour être courants et vérifiables, tels que les robots d'exploration des moteurs de recherche connus, ne sont pas soumis aux actions que vous définissez ici. Le contrôle des bots confirme que les bots validés proviennent de la source indiquée avant de les marquer comme vérifiés.

Pour configurer la protection d’une catégorie de bot

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez modifier.
3. Choisissez l’onglet Security (Sécurité).
4. Dans le graphique Catégories de demandes par bot, pointez sur l’un des éléments de la colonne Action de bot non vérifiée et choisissez l’icône en forme de crayon pour le modifier.
5. Ouvrez la liste obtenue et choisissez l'un des éléments suivants :
   - Bloc
   - Allow
   - Mode de surveillance
   - CAPTCHA
   - Défi
6. Cochez la case à côté de la liste pour enregistrer votre modification.

Gérer AWS WAF protections de sécurité dans le tableau de bord CloudFront de sécurité

CloudFront crée un tableau de bord de sécurité pour chacune de vos distributions. Vous utilisez les tableaux de bord de la CloudFront console. Grâce aux tableaux de bord, vous pouvez les utiliser CloudFront et les AWS WAF regrouper en un seul endroit pour surveiller et gérer les protections de sécurité courantes pour vos applications Web. Les tableaux de bord fournissent les tâches et les données suivantes :

- Configuration de la sécurité : vous pouvez activer et désactiver les AWS WAF protections, et consulter toutes les protections spécifiques à l'application, telles que WordPress les protections.
- Tendances en matière de sécurité : elles incluent les demandes autorisées et bloquées, les demandes de type défi et CAPTCHA, ainsi que les principaux types d'attaques. Vous pouvez voir les ratios de trafic et leur évolution au fil du temps. Par exemple, si toutes les demandes augmentent de 3 %, mais que les demandes autorisées augmentent de 14 %, cela signifie que vous avez autorisé une plus grande partie de votre trafic au cours de la période en cours.
- Demandes de bot : vous pouvez voir quelle quantité de trafic provient des bots, quels types de bots (vérifiés ou non vérifiés) et comment les pourcentages de répartition des types de bots (vérifiés ou non vérifiés) évoluent au fil du temps. Pour plus d'informations sur l'activation du contrôle des bots, consultez Activation du contrôle des bots.
- Journaux de demandes : les données des journaux peuvent aider à répondre aux questions concernant les tendances en matière de sécurité ou les demandes de bots. Vous pouvez effectuer des recherches dans vos journaux sans écrire de requêtes et consulter des graphiques agrégés pour déterminer si un ensemble de journaux filtré est principalement piloté par un sous-ensemble de méthodes HTTP, d'adresses IP, de chemins d'URI ou de pays. Vous pouvez survoler les valeurs des graphiques et bloquer les adresses IP et les pays. Pour plus d'informations, consultez Enable AWS WAF journaux.
- Gestion des restrictions géographiques — CloudFront et AWS WAF fourniture de fonctionnalités de restriction géographique. CloudFront fournit des restrictions géographiques gratuitement, mais les statistiques relatives aux restrictions CloudFront géographiques ne sont pas affichées dans le tableau de bord de sécurité. Pour consulter les statistiques relatives aux demandes de pays bloquées, vous devez utiliser des restrictions AWS WAF géographiques. Pour ce faire, survolez la barre correspondant à un pays dans le tableau de bord de sécurité et bloquez ce pays. Pour plus d'informations, consultez Utiliser des restrictions CloudFront géographiques.

- L'option Bloquer n'est peut-être pas disponible si vous avez déjà créé une AWS WAF règle personnalisée en dehors de la CloudFront console pour bloquer des pays.

Rubriques

- Conditions préalables
- Enable AWS WAF journaux

Conditions préalables

Vous devez l'activer AWS WAF si vous souhaitez afficher les mesures de sécurité dans le tableau de bord CloudFront de sécurité. Si vous ne l'activez pas AWS WAF, vous pouvez uniquement utiliser le tableau de bord Sécurité pour activer AWS WAF ou configurer les restrictions CloudFront géographiques.

Pour plus d'informations sur l'activation AWS WAF, consultezEnable AWS WAF pour les distributions.

Enable AWS WAF journaux

AWS WAF les données de journal peuvent vous aider à isoler des modèles de trafic spécifiques. Par exemple, les journaux peuvent vous indiquer d'où provient un certain trafic ou ce qu'il fait.

Si vous activez la AWS WAF connexion à CloudWatch, le tableau CloudFront de bord de sécurité interroge, regroupe et affiche les informations issues des CloudWatch journaux. L'utilisation du tableau de bord de sécurité est gratuite, mais la CloudWatch tarification s'applique aux journaux interrogés via le tableau de bord. Pour plus d'informations, consultez la page CloudWatch Tarification Amazon.

Pour activer la journalisation

1. Entrez le volume de demandes attendu dans la requests/month case Nombre pour estimer les coûts liés à l'activation des journaux.
2. Cochez la case Activer les AWS WAF journaux.
3. Sélectionnez Activer.

CloudFront crée un groupe de CloudWatch journaux et met à jour votre AWS WAF configuration pour commencer à vous connecter CloudWatch. Lors de la première utilisation, plusieurs minutes peuvent s'écouler avant que les données du journal s'affichent. La section Demandes du graphique répertorie

chaque demande. Sous les demandes individuelles, le graphique à barres regroupe les données par méthode HTTP, les principaux chemins d'URI, les principales adresses IP et les principaux pays. Les graphiques peuvent vous aider à repérer des schémas. Par exemple, vous pouvez voir un volume disproportionné de demandes provenant d'une seule adresse IP ou de données provenant d'un pays que vous n'avez encore jamais vu dans vos journaux. Vous pouvez filtrer les demandes en fonction du pays, de l'en-tête de l'hôte et d'autres attributs afin de détecter le trafic indésirable. Après avoir identifié ce trafic, passez la souris sur une requête individuelle ou un élément du graphique et bloquez une adresse IP ou un pays.

> **Note**
>
> Les métriques affichées sont basées sur l'ACL web. Par conséquent, si vous associez la même ACL Web à plusieurs distributions, vous verrez toutes les mesures relatives à votre ACL Web, et pas seulement les AWS WAF demandes traitées pour cette distribution.

Configuration de la limitation du débit

La limitation du débit fait partie des recommandations que vous pouvez recevoir lors de la configuration des protections de sécurité.

CloudFront active toujours la limitation de débit en mode moniteur. Lorsque le mode moniteur est activé, CloudFront capture les mesures qui vous indiquent si le taux que vous avez configuré dans le champ Limitation du débit a été dépassé, à quelle fréquence et dans quelle mesure.

Après avoir enregistré la distribution, CloudFront commence à collecter des données en fonction du nombre indiqué dans le champ Limitation du débit.

Vous pouvez activer ou gérer les paramètres de limitation de débit dans la section Sécurité - Web Application Firewall (WAF) de l'onglet Sécurité de n'importe quelle CloudFront distribution.

> **Note**
>
> L'option Limitation du débit n'apparaît dans la CloudFront console que si vous avez spécifié une origine personnalisée autre que S3 pour votre distribution. Dans le cas contraire, seules les protections principales activées pour la distribution seront affichées. Pour plus d'informations sur les types d'origine, consultez Utilisez différentes origines avec les CloudFront distributions.

Pour configurer la limitation du débit

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis sélectionnez la distribution que vous souhaitez modifier.
3. Choisissez l'onglet Security (Sécurité).
4. Dans la section Sécurité – Pare-feu d'application web (WAF), sélectionnez Modifier.
5. Sous Protections supplémentaires, sélectionnez Limitation du débit. Vous pouvez éventuellement modifier la limite de débit. Lorsque vous avez optimisé le débit avec précision, choisissez Enregistrer les modifications.
6. Dans la section Sécurité — Pare-feu pour applications Web (WAF), à côté de Limitation du débit, vous pouvez choisir le mode moniteur, puis activer le blocage pour désactiver le mode surveillance. CloudFront commencera à bloquer les demandes qui dépassent la limite de débit spécifiée.

Pour plus d'informations sur l'activation AWS WAF et la limitation du débit, consultez le billet de blog Présentation du tableau de bord de CloudFront sécurité, un CDN unifié et une expérience de sécurité.

Désactiver AWS WAF protections de sécurité

Si votre distribution n'a pas besoin AWS WAF de protections de sécurité, vous pouvez désactiver cette fonctionnalité à l'aide de la CloudFront console.

Si vous avez précédemment activé AWS WAF la protection et que vous n'avez pas choisi de configuration WAF existante (également appelée protection à choix unique), vous avez CloudFront automatiquement créé une ACL Web pour vous. Pour les ACL Web créées de cette manière, la CloudFront console dissocie la ressource et supprime l'ACL Web.

La dissociation d'une ACL web est différente de sa suppression. La dissociation retire l'ACL web de votre distribution, mais elle n'est pas supprimée de votre Compte AWS. Pour plus d'informations, consultez Associer ou dissocier une ACL Web à une AWS ressource dans le AWS WAF AWS Firewall Manager, et AWS Shield Advanced le Guide du développeur.

Consultez la procédure suivante pour désactiver les AWS WAF protections et dissocier l'ACL Web de votre distribution.

Pour désactiver AWS WAF protections de sécurité dans CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis sélectionnez la distribution que vous souhaitez modifier.
3. Choisissez l'onglet Sécurité, puis sélectionnez Modifier.
4. Dans la section Web Application Firewall (WAF), choisissez Désactiver AWS WAF la protection.
5. Cliquez sur Enregistrer les modifications.

Remarques

- Si vous avez désactivé AWS WAF la protection de sécurité et que vous souhaitez toujours supprimer l'ACL Web de votre Compte AWS compte, vous pouvez la supprimer manuellement. Suivez la procédure pour supprimer une ACL web. Dans la console AWS WAF & Shield, pour la page ACL Web, vous devez choisir la liste globale (CloudFront) pour trouver les ACL Web.
- Lorsque vous supprimez une distribution de la CloudFront console, vous CloudFront tenterez également de supprimer l'ACL Web si vous avez choisi une protection à choix unique. L'opération est effectuée dans la mesure du possible, sans garantie absolue. Pour plus d'informations, consultez Supprimer une distribution.

Configuration d’un accès sécurisé et restriction de l’accès au contenu

CloudFront propose plusieurs options pour sécuriser le contenu qu'il diffuse. Voici quelques moyens que vous pouvez utiliser CloudFront pour sécuriser et restreindre l'accès au contenu :

- Configurer les connexions HTTPS.
- Empêcher les utilisateurs situés dans des points géographiques spécifiques d’accéder au contenu
- Exiger des utilisateurs qu'ils accèdent au contenu à l'aide d'URL CloudFront signées ou de cookies signés
- Configurer le chiffrement au niveau du champ pour des champs de contenu spécifiques
- AWS WAF À utiliser pour contrôler l'accès à votre contenu

Vous devez également implémenter une DDoS-resilient architecture pour votre infrastructure et vos applications. Pour plus d’informations, consultez Bonnes pratiques AWS pour la résistance aux attaques DDoS.

Pour plus d'informations, consultez les éléments suivants :

- Sécurisez la diffusion de votre contenu avec CloudFront
- SIEM sur Amazon Service OpenSearch

Rubriques

- Utilisez le protocole HTTPS avec CloudFront
- Utilisation de noms de domaines alternatifs et HTTPS
- Authentification TLS mutuelle avec CloudFront (Viewer MTLS)
- TLS mutuel d'origine avec CloudFront
- Offre de contenu privé avec des URL et des cookies signés
- Restreindre l'accès à un AWS origine
- Restriction de l’accès aux Application Load Balancers
- Restriction de la distribution géographique de votre contenu
- Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles

Utilisez le protocole HTTPS avec CloudFront

Vous pouvez configurer CloudFront pour exiger que les spectateurs utilisent le protocole HTTPS afin que les connexions soient cryptées lors des CloudFront communications avec les spectateurs. Vous pouvez également CloudFront configurer l'utilisation du protocole HTTPS avec votre origine afin que les connexions soient chiffrées lorsque CloudFront vous communiquez avec votre origine.

Si vous configurez CloudFront le protocole HTTPS pour communiquer à la fois avec les spectateurs et pour communiquer avec votre origine, voici ce qui se passe lorsque CloudFront vous recevez une demande :

1. Un utilisateur envoie une requête HTTPS à CloudFront. Il y a ici une certaine SSL/TLS négociation entre le spectateur et CloudFront. La visionneuse finit par envoyer la requête dans un format chiffré.
2. Si l'emplacement CloudFront périphérique contient une réponse mise en cache, CloudFront chiffre la réponse et la renvoie au visualiseur, qui la déchiffre.
3. Si l'emplacement CloudFront périphérique ne contient pas de réponse mise en cache, CloudFront effectue une SSL/TLS négociation avec votre origine et, une fois la négociation terminée, transmet la demande à votre origine dans un format crypté.
4. Votre origine déchiffre la demande, la traite (génère une réponse), chiffre la réponse et renvoie la réponse à. CloudFront
5. CloudFront déchiffre la réponse, la rechiffre et la transmet au spectateur. CloudFrontmet également la réponse en cache à l'emplacement périphérique afin qu'elle soit disponible la prochaine fois qu'elle sera demandée.
6. La visionneuse déchiffre la réponse.

Le processus fonctionne essentiellement de la même manière, MediaStore que votre origine soit un compartiment Amazon S3 ou une origine personnalisée telle qu'un HTTP/S serveur.

> **Note**
>
> Pour aider à contrecarrer les attaques de type renégociation SSL, CloudFront ne prend pas en charge la renégociation pour les requêtes d'utilisateur et d'origine.

Vous pouvez également activer l'authentification mutuelle pour votre CloudFront distribution. Pour plus d’informations, consultez Authentification TLS mutuelle avec CloudFront (Viewer MTLS).

Pour plus d'informations sur la manière d'exiger le protocole HTTPS entre les spectateurs et CloudFront, CloudFront et entre et votre origine, consultez les rubriques suivantes.

Rubriques

- Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront
- Exiger le protocole HTTPS pour la communication entre CloudFront et votre origine personnalisée
- Exiger le protocole HTTPS pour les communications entre CloudFront et votre origine Amazon S3
- Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront
- Protocoles et chiffrements pris en charge entre CloudFront et l'origine

Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront

Vous pouvez configurer un ou plusieurs comportements de cache dans votre CloudFront distribution pour exiger le protocole HTTPS pour les communications entre les spectateurs et CloudFront. Vous pouvez également configurer un ou plusieurs comportements de cache pour autoriser à la fois le HTTP et le HTTPS, ce qui CloudFront nécessite le protocole HTTPS pour certains objets mais pas pour d'autres. Les étapes de configuration dépendent du nom de domaine que vous utilisez dans les URL d'objet :

- Si vous utilisez le nom de domaine CloudFront attribué à votre distribution, tel que d111111abcdef8.cloudfront.net, vous modifiez le paramètre Viewer Protocol Policy pour un ou plusieurs comportements de cache afin de nécessiter une communication HTTPS. Dans cette configuration, CloudFront fournit le SSL/TLS certificat.

  Pour modifier la valeur de Viewer Protocol Policy à l'aide de la CloudFront console, reportez-vous à la procédure décrite plus loin dans cette section.

  Pour plus d'informations sur l'utilisation de l' CloudFront API pour modifier la valeur de l'`ViewerProtocolPolicy`élément, consultez UpdateDistribution le manuel Amazon CloudFront API Reference.
- Si vous utilisez votre propre nom de domaine, comme example.com, vous devez modifier plusieurs paramètres CloudFront. Vous devez également utiliser un SSL/TLS certificat fourni par AWS Certificate Manager (ACM) ou importer un certificat d'une autorité de certification tierce vers ACM ou le magasin de certificats IAM. Pour plus d’informations, consultez Utilisation de noms de domaines alternatifs et HTTPS.

> **Note**
>
> Si vous voulez vous assurer que les objets que les spectateurs obtiennent CloudFront étaient chiffrés lorsqu'ils les ont CloudFront obtenus depuis votre origine, utilisez toujours le protocole HTTPS entre CloudFront et votre origine. Si vous êtes récemment passé du protocole HTTP au protocole HTTPS entre CloudFront et votre origine, nous vous recommandons d'invalider les objets situés dans des emplacements CloudFront périphériques. CloudFront renverra un objet à un visualiseur, que le protocole utilisé par le visualiseur (HTTP ou HTTPS) corresponde ou non à celui CloudFront utilisé pour obtenir l'objet. Pour plus d'informations sur la suppression ou le remplacement des objets dans une distribution, consultez Ajouter, supprimer ou remplacer le contenu qui CloudFront distribue.

Exigence du protocole HTTPS pour les utilisateurs

Pour exiger le protocole HTTPS entre les spectateurs et CloudFront pour un ou plusieurs comportements de cache, effectuez la procédure suivante.

Pour configurer CloudFront pour exiger le protocole HTTPS entre les spectateurs et CloudFront

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet supérieur de la CloudFront console, choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Dans l'onglet Comportements, choisissez le comportement de cache à mettre à jour, puis sélectionnez Modifier.
4. Spécifiez l'une des valeurs suivantes pour Politique de protocole d'utilisateur :

   Redirect HTTP to HTTPS

   Les visionneuses peuvent utiliser les deux protocoles. Le protocole HTTP `GET` et les `HEAD` requêtes sont automatiquement redirigés vers les requêtes HTTPS. CloudFront renvoie le code d'état HTTP 301 (Déplacé définitivement) ainsi que la nouvelle URL HTTPS. L'utilisateur soumet ensuite à nouveau la demande à CloudFront l'aide de l'URL HTTPS.

> **Important**
>
> Si vous envoyez`POST`, `PUT` `DELETE``OPTIONS`, ou `PATCH` via HTTP avec un comportement de cache HTTP vers HTTPS et une version du protocole de requête HTTP 1.1 ou supérieure, CloudFront redirige la demande vers un emplacement HTTPS avec un code d'état HTTP 307 (redirection temporaire). Cette approche garantit le nouvel envoi de la demande vers le nouvel emplacement à l'aide de la même méthode et de la même charge utile du corps.
> Si vous envoyez`POST`, `PUT` `DELETE``OPTIONS`, ou des `PATCH` requêtes via HTTP vers un comportement de cache HTTPS avec une version du protocole de requête inférieure à HTTP 1.1, CloudFront renvoie un code d'état HTTP 403 (Interdit).

Quand un utilisateur émet une requête HTTP redirigée vers une requête HTTPS, CloudFront perçoit des frais pour les deux requêtes. Pour la requête HTTP, les frais ne concernent que la demande et les en-têtes renvoyés au visualiseur. CloudFront Pour la requête HTTPS, le montant correspond à la requête ainsi qu'aux en-têtes et à l'objet renvoyés par votre origine.

HTTPS Only

Les visionneuses ne peuvent accéder au contenu que si elles utilisent le protocole HTTPS. Si un utilisateur envoie une requête HTTP au lieu d'une requête HTTPS, il CloudFront renvoie le code d'état HTTP 403 (Interdit) et ne renvoie pas l'objet.

5. Cliquez sur Enregistrer les modifications.
6. Répétez les étapes 3 à 5 pour chaque comportement de cache supplémentaire pour lequel vous souhaitez exiger le protocole HTTPS entre les spectateurs et CloudFront.
7. Vérifiez les éléments suivants avant d’utiliser la configuration mise à jour dans un environnement de production :

   - Le modèle de chemin de chaque comportement de cache s’applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
   - Les comportements du cache sont répertoriés dans l'ordre dans lequel vous CloudFront souhaitez les évaluer. Pour plus d’informations, consultez Modèle de chemin.
   - Les comportements de cache acheminent les requêtes vers les origines correctes.

Exiger le protocole HTTPS pour la communication entre CloudFront et votre origine personnalisée

Vous pouvez avoir besoin du protocole HTTPS pour les communications entre CloudFront et votre pays d'origine.

> **Note**
>
> Si votre origine est un compartiment Amazon S3 configuré comme point de terminaison de site Web, vous ne pouvez pas configurer CloudFront pour utiliser HTTPS avec votre origine car Amazon S3 ne prend pas en charge le protocole HTTPS pour les points de terminaison de site Web.

Pour exiger le protocole HTTPS entre CloudFront et votre origine, suivez les procédures décrites dans cette rubrique pour effectuer les opérations suivantes :

1. Dans votre distribution, modifiez le paramètre Stratégie de protocole d'origine pour l'origine.
2. Installez un SSL/TLS certificat sur votre serveur d'origine (cela n'est pas obligatoire lorsque vous utilisez une origine Amazon S3 ou certaines autres AWS origines).

Rubriques

- Exigence du protocole HTTPS pour les origines personnalisées
- Installez un SSL/TLS certificat sur votre origine personnalisée

Exigence du protocole HTTPS pour les origines personnalisées

La procédure suivante explique comment configurer l'utilisation du protocole HTTPS CloudFront pour communiquer avec un équilibreur de charge Elastic Load Balancing, une instance Amazon EC2 ou une autre origine personnalisée. Pour plus d'informations sur l'utilisation de l' CloudFront API pour mettre à jour une distribution, consultez UpdateDistribution le manuel Amazon CloudFront API Reference.

Pour configurer CloudFront pour exiger le protocole HTTPS entre CloudFront et votre origine personnalisée

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet supérieur de la CloudFront console, choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Dans l'onglet Origines, sélectionnez l'origine que vous souhaitez mettre à jour, puis choisissez Modifier.
4. Modifiez les paramètres suivants :

   Origin Protocol Policy

   Modifiez le paramètre Stratégie de protocole d'origine pour les origines concernées de votre distribution :

   - HTTPS uniquement : CloudFront utilise uniquement le protocole HTTPS pour communiquer avec votre origine personnalisée.
   - Match Viewer : CloudFront communique avec votre origine personnalisée via HTTP ou HTTPS, selon le protocole de la demande du visualiseur. Par exemple, si vous choisissez Match Viewer pour la politique de protocole d'origine et que le visualiseur utilise HTTPS pour demander un objet CloudFront, utilise CloudFront également HTTPS pour transmettre la demande à votre origine.

     Ne sélectionnez Identique à l’utilisateur que si vous affectez la valeur Rediriger HTTP vers HTTPS ou HTTPS uniquement au paramètre Stratégie de protocole d’utilisateur.

     CloudFront met l'objet en cache une seule fois, même si les utilisateurs font des requêtes en utilisant à la fois les protocoles HTTP et HTTPS.

   Origin SSL Protocols

   Choisissez les Protocoles SSL d'origine pour les origines concernées de votre distribution. Le protocole SSLv3 étant moins sécurisé, nous vous recommandons de choisir SSLv3 uniquement si votre origine ne prend pas en charge TLSv1 ou version ultérieure. Le handshake TLSv1 est à la fois rétrocompatible et rétrocompatible avec SSLv3, mais TLSv1.1 les versions ultérieures ne le sont pas. Lorsque vous choisissez SSLv3, CloudFront seules les demandes d'établissement de liaison SSLv3 sont envoyées.
5. Cliquez sur Enregistrer les modifications.

6. Répétez les étapes 3 à 5 pour chaque origine supplémentaire pour laquelle vous souhaitez exiger le protocole HTTPS entre CloudFront et votre origine personnalisée.
7. Vérifiez les éléments suivants avant d'utiliser la configuration mise à jour dans un environnement de production :

   - Le modèle de chemin de chaque comportement de cache s'applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
   - Les comportements du cache sont répertoriés dans l'ordre dans lequel vous CloudFront souhaitez les évaluer. Pour plus d'informations, consultez Modèle de chemin.
   - Les comportements de cache acheminent les requêtes vers les origines pour lesquelles vous avez modifié le paramètre Stratégie de protocole d'origine.

Installez un SSL/TLS certificat sur votre origine personnalisée

Vous pouvez utiliser un SSL/TLS certificat provenant des sources suivantes sur votre origine personnalisée :

- Si votre origine est un équilibreur de charge Elastic Load Balancing, vous pouvez utiliser un certificat fourni par AWS Certificate Manager (ACM). Vous pouvez également utiliser un certificat signé par une autorité de certification tierce reconnue et importé dans ACM.
- Pour les origines autres que les équilibreurs de charge Elastic Load Balancing, vous devez utiliser un certificat signé par une autorité de certification (CA) tierce de confiance, par exemple Comodo ou DigiCert Symantec.

Le certificat renvoyé depuis l'origine doit comprendre l'un des noms de domaine suivants :

- Le nom de domaine dans le champ Domaine d'origine de l'origine (le `DomainName` champ de l' CloudFront API).
- Nom du domaine dans l'en-tête `Host`, si le comportement du cache est configuré pour transférer l'en-tête `Host` de l'origine.

Lorsque CloudFront utilise le protocole HTTPS pour communiquer avec votre origine, CloudFront vérifie que le certificat a été émis par une autorité de certification fiable. CloudFront prend en charge les mêmes autorités de certification que Mozilla. Pour obtenir la liste actuelle, consultez Liste des certificats CA inclus dans Mozilla. Vous ne pouvez pas utiliser de certificat auto-signé pour les communications HTTPS entre CloudFront et votre origine.

> **Important**
>
> Si le serveur d'origine renvoie un certificat expiré, un certificat non valide ou un certificat auto-signé, ou s'il renvoie la chaîne de certificats dans le mauvais ordre, interrompt la CloudFront connexion TCP, renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur et définit l'`X-Cache`en-tête sur. `Error from cloudfront` De plus, si la chaîne complète de certificats, y compris le certificat intermédiaire, n'est pas présente, la connexion TCP est CloudFront interrompue.

Exiger le protocole HTTPS pour les communications entre CloudFront et votre origine Amazon S3

Lorsque votre origine est un compartiment Amazon S3, vos options d'utilisation du protocole HTTPS pour les communications CloudFront dépendent de la manière dont vous utilisez le compartiment. Si votre compartiment Amazon S3 est configuré comme point de terminaison de site Web, vous ne pouvez pas le configurer CloudFront pour utiliser le protocole HTTPS pour communiquer avec votre point d'origine, car Amazon S3 ne prend pas en charge les connexions HTTPS dans cette configuration.

Lorsque votre origine est un compartiment Amazon S3 qui prend en charge la communication HTTPS, il CloudFront transmet les demandes à S3 en utilisant le protocole utilisé par les spectateurs pour soumettre les demandes. La valeur par défaut du paramètre Protocole (origines personnalisées uniquement) est Identique à l'utilisateur et elle ne peut pas être modifiée. Toutefois, si vous activez le contrôle d'accès à l'origine (OAC) pour votre Amazon S3 origin, la communication utilisée entre CloudFront et Amazon S3 dépend de vos paramètres. Pour plus d'informations, consultez Création d'un nouveau contrôle d'accès d'origine.

Si vous souhaitez exiger le protocole HTTPS pour les communications entre CloudFront et Amazon S3, vous devez modifier la valeur de Viewer Protocol Policy pour qu'elle redirige HTTP vers HTTPS ou HTTPS uniquement. La procédure décrite plus loin dans cette section explique comment utiliser la CloudFront console pour modifier la politique du protocole Viewer. Pour plus d'informations sur l'utilisation de l' CloudFront API pour mettre à jour l'`ViewerProtocolPolicy`élément d'une distribution, consultez UpdateDistribution le manuel Amazon CloudFront API Reference.

Lorsque vous utilisez le protocole HTTPS avec un compartiment Amazon S3 qui prend en charge la communication HTTPS, Amazon S3 fournit le SSL/TLS certificat, vous n'avez donc pas à le faire.

Exigence du protocole HTTPS pour une origine Amazon S3

La procédure suivante vous montre comment configurer CloudFront pour exiger le protocole HTTPS sur votre origine Amazon S3.

Pour configurer CloudFront afin d'exiger le protocole HTTPS sur votre origine Amazon S3

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet supérieur de la CloudFront console, choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Sous l'onglet Comportements, choisissez le comportement de cache à mettre à jour, puis cliquez sur Modifier.
4. Spécifiez l'une des valeurs suivantes pour Politique de protocole d'utilisateur :

   Redirect HTTP to HTTPS

   Les utilisateurs peuvent utiliser les deux protocoles, mais les requêtes HTTP sont automatiquement redirigées vers les requêtes HTTPS. CloudFront renvoie le code d'état HTTP 301 (Déplacé définitivement) ainsi que la nouvelle URL HTTPS. L'utilisateur soumet ensuite à nouveau la demande à CloudFront l'aide de l'URL HTTPS.

   > **Important**
   >
   > CloudFront ne redirige pas `DELETEOPTIONS`, `PATCHPOST`, ou les `PUT` requêtes de HTTP vers HTTPS. Si vous configurez un comportement de cache pour rediriger vers HTTPS, CloudFront répondez à `HTTPDELETE`,`OPTIONS`, `PATCHPOST`, ou à des `PUT` demandes concernant ce comportement de cache avec le code d'état HTTP 403 (Interdit).

   Quand un utilisateur émet une requête HTTP redirigée vers une requête HTTPS, CloudFront perçoit des frais pour les deux requêtes. Pour la requête HTTP, les frais ne concernent que la demande et les en-têtes renvoyés au visualiseur. CloudFront Pour la requête HTTPS, le montant correspond à la requête ainsi qu'aux en-têtes et à l'objet renvoyés par votre origine.

HTTPS Only

Les visionneuses ne peuvent accéder au contenu que si elles utilisent le protocole HTTPS. Si un utilisateur envoie une requête HTTP au lieu d'une requête HTTPS, il CloudFront renvoie le code d'état HTTP 403 (Interdit) et ne renvoie pas l'objet.

5. Choisissez Oui, Modifier.
6. Répétez les étapes 3 à 5 pour chaque comportement de cache supplémentaire pour lequel vous souhaitez exiger le protocole HTTPS entre les spectateurs et CloudFront, et entre CloudFront et S3.
7. Vérifiez les éléments suivants avant d'utiliser la configuration mise à jour dans un environnement de production :

   - Le modèle de chemin de chaque comportement de cache s'applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
   - Les comportements du cache sont répertoriés dans l'ordre dans lequel vous CloudFront souhaitez les évaluer. Pour plus d'informations, consultez Modèle de chemin.
   - Les comportements de cache acheminent les requêtes vers les origines correctes.

Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront

Lorsque vous avez besoin du protocole HTTPS entre les spectateurs et votre CloudFront diffusion, vous devez choisir une politique de sécurité qui détermine les paramètres suivants :

- SSL/TLS Protocole minimal CloudFront utilisé pour communiquer avec les spectateurs.
- Chiffres que CloudFront vous pouvez utiliser pour crypter la communication avec les spectateurs.

Pour choisir une stratégie de sécurité, spécifiez la valeur applicable pour Politique de sécurité (SSL/TLS version minimale). Le tableau suivant répertorie les protocoles et chiffrements que CloudFront vous pouvez utiliser pour chaque politique de sécurité.

Un utilisateur doit prendre en charge au moins l'un des chiffrements pris en charge pour établir une connexion HTTPS avec. CloudFront CloudFront choisit un chiffrement dans l'ordre indiqué parmi les chiffrements pris en charge par le visualiseur. Consultez également Noms de chiffrement OpenSSL, s2n et RFC.

	Stratégie de sécurité								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
SSL/TLS Protocoles pris en charge									
TLSv1.3	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLSv1.2	♦	♦	♦	♦	♦	♦	♦	♦	
TLSv1.1	♦	♦	♦	♦					
TLSv1	♦	♦	♦						
SSLv3	♦								
TLSv1.3 Chiffrements pris en charge									
TLS_AES_128_GCM_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_AES_256_GCM_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_CHACHA20_POLY1305_SHA256	♦	♦	♦	♦	♦	♦	♦		♦
Chiffrements ECDSA pris en charge									
ECDHE-ECDSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-AES128-SHA256	♦	♦	♦	♦	♦	♦			
ECDHE-ECDSA-AES128-SHA	♦	♦	♦	♦					

	Stratégie de sécurité								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
ECDHE-ECDSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-ECDSA-CHACHA20-POLY1305	♦	♦	♦	♦	♦	♦	♦		
ECDHE-ECDSA-AES256-SHA384	♦	♦	♦	♦	♦	♦			
ECDHE-ECDSA-AES256-SHA	♦	♦	♦	♦					
Chiffrements RSA pris en charge									
ECDHE-RSA-AES128-GCM-SHA256	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-RSA-AES128-SHA256	♦	♦	♦	♦	♦	♦			
ECDHE-RSA-AES128-SHA	♦	♦	♦	♦					
ECDHE-RSA-AES256-GCM-SHA384	♦	♦	♦	♦	♦	♦	♦	♦	
ECDHE-RSA-CHACHA20-POLY1305	♦	♦	♦	♦	♦	♦	♦		

	Stratégie de sécurité								
	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
ECDHE-RSA-AES256-SHA384	♦	♦	♦	♦	♦	♦			
ECDHE-RSA-AES256-SHA	♦	♦	♦	♦					
AES128-GCM-SHA256	♦	♦	♦	♦	♦				
AES256-GCM-SHA384	♦	♦	♦	♦	♦				
AES128-SHA256	♦	♦	♦	♦	♦				
AES256-SHA	♦	♦	♦	♦					
AES128-SHA	♦	♦	♦	♦					
DES-CBC3-SHA	♦	♦							
RC4-MD5	♦								

Noms de chiffrement OpenSSL, s2n et RFC

OpenSSL et s2n utilisent des noms de chiffrement différents de ceux utilisés par les standards TLS (RFC 2246, RFC 4346, RFC 5246, et RFC 8446). Le tableau suivant met en correspondance les noms OpenSSL et s2n avec le nom RFC pour chaque chiffrement.

CloudFront prend en charge les échanges de clés classiques et quantiques sécurisés. Pour les échanges de clés classiques utilisant des courbes elliptiques, CloudFront prend en charge les options suivantes :

- `prime256v1`
- `X25519`

- `secp384r1`

Pour les échanges de clés quantiques sécurisés, prend en CloudFront charge les éléments suivants :

- `X25519MLKEM768`
- `SecP256r1MLKEM768`

> **Note**
>
> Quantum-safe les échanges de clés ne sont pris en charge qu'avec TLS 1.3. Les versions TLS 1.2 et antérieures ne prennent pas en charge les échanges de clés sécurisés quantiques.

Pour plus d’informations, consultez les rubriques suivantes :

- Post-Quantum Cryptographie
- Algorithmes de cryptographie et Services AWS
- Échange de clés hybride dans TLS 1.3

Pour plus d'informations sur les exigences en matière de certificat pour CloudFront, consultezExigences relatives à l'utilisation de SSL/TLS certificats avec CloudFront.

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
TLSv1.3 Chiffrements pris en charge	
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256
Chiffrements ECDSA pris en charge	
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-ECDSA-CHACHA20-POLY1305	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
Chiffrements RSA pris en charge	
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-CHACHA20-POLY1305	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5

Schémas de signature pris en charge entre les spectateurs et CloudFront

CloudFront prend en charge les schémas de signature suivants pour les connexions entre les spectateurs etCloudFront.

	Politique de sécurité								
Schémas de signature	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦

	Politique de sécurité								
Schémas de signature	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_SIGNATURE_SCHEME_RSA_PSS_PSS_SHA512	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PSS_RSAE_SHA512	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦

	Politique de sécurité								
Schémas de signature	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA512	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA224	♦	♦	♦	♦	♦	♦	♦		
TLS_SIGNATURE_SCHEME_ECDSA_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_ECDSA_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_ECDSA_SHA512	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_ECDSA_SHA224	♦	♦	♦	♦	♦	♦	♦		
TLS_SIGNATURE_SCHEME_ECDSA_SECP256R1_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦

	Politique de sécurité								
Schémas de signature	SSLv3	TLSv1	TLSv1_6	TLSv1.016	TLSv1.018	TLSv1.019	TLSv1.021	TLSv1.025	TLSv1.3_2025
TLS_SIGNATURE_SCHEME_ECDSA_SECP384R1_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA1	♦	♦	♦	♦					
TLS_SIGNATURE_SCHEME_ECDSA_SHA1	♦	♦	♦	♦					

Protocoles et chiffrements pris en charge entre CloudFront et l'origine

Si vous choisissez d'exiger le protocole HTTPS entre CloudFront et votre origine, vous pouvez choisir le SSL/TLS protocole à autoriser pour la connexion sécurisée et CloudFront vous connecter à l'origine à l'aide de l'un des chiffrements ECDSA ou RSA répertoriés dans le tableau suivant. Votre origine doit prendre en charge au moins l'un de ces chiffrements pour CloudFront établir une connexion HTTPS avec votre origine.

OpenSSL et s2n utilisent des noms de chiffrement différents de ceux utilisés par les standards TLS (RFC 2246, RFC 4346, RFC 5246, et RFC 8446). Le tableau suivant inclut les noms OpenSSL et s2n avec le nom RFC pour chaque chiffrement.

Pour les chiffrements utilisant des algorithmes d'échange de clés à courbe elliptique, CloudFront prend en charge les courbes elliptiques suivantes :

- prime256v1
- secp384r1
- X25519

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
Chiffrements ECDSA pris en charge	
ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ECDHE-ECDSA-AES256-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ECDHE-ECDSA-AES128-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ECDHE-ECDSA-AES128-SHA	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
Chiffrements RSA pris en charge	
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES256-SHA384	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES128-SHA256	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Nom de chiffrement OpenSSL et s2n	Nom de chiffrement RFC
ECDHE-RSA-AES128-SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5	TLS_RSA_WITH_RC4_128_MD5

Schémas de signature pris en charge entre CloudFront et l'origine

CloudFront prend en charge les schémas de signature suivants pour les connexions entre CloudFront et l'origine.

- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA256
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA384
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA512
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA224
- TLS_SIGNATURE_SCHEME_ECDSA_SHA256
- TLS_SIGNATURE_SCHEME_ECDSA_SHA384
- TLS_SIGNATURE_SCHEME_ECDSA_SHA512
- TLS_SIGNATURE_SCHEME_ECDSA_SHA224
- TLS_SIGNATURE_SCHEME_RSA_PKCS1_SHA1
- TLS_SIGNATURE_SCHEME_ECDSA_SHA1

Utilisation de noms de domaines alternatifs et HTTPS

Si vous souhaitez employer votre propre nom de domaine dans les URL de vos fichiers (comme `https://www.example.com/image.jpg`) et que vous voulez que vos utilisateurs utilisent le protocole HTTPS, vous devez réaliser les étapes décrites dans les rubriques suivantes. (Si vous utilisez le nom de domaine de CloudFront distribution par défaut dans vos URL, par

exemple`https://d111111abcdef8.cloudfront.net/image.jpg`, suivez plutôt les instructions de la rubrique suivante :Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.)

> **Important**
>
> Lorsque vous ajoutez un certificat à votre distribution, le certificat se propage CloudFront immédiatement à tous ses emplacements périphériques. Tandis que de nouveaux emplacements périphériques deviennent disponibles, CloudFront leur transmet également le certificat. Vous ne pouvez pas limiter les emplacements périphériques vers lesquels les CloudFront certificats se propagent.

Rubriques

- Choisissez la manière dont CloudFront les requêtes HTTPS sont traitées
- Exigences relatives à l'utilisation de SSL/TLS certificats avec CloudFront
- Quotas d'utilisation de SSL/TLS certificats avec CloudFront (HTTPS entre spectateurs et CloudFront uniquement)
- Configuration de noms de domaines alternatifs et HTTPS
- Déterminer la taille de la clé publique dans un certificat SSL/TLS RSA
- Augmenter les quotas de SSL/TLS certificats
- Rotation SSL/TLS des certificats
- Revenir d'un SSL/TLS certificat personnalisé au certificat par défaut CloudFront
- Passez d'un SSL/TLS certificat personnalisé avec des adresses IP dédiées au SNI

Choisissez la manière dont CloudFront les requêtes HTTPS sont traitées

Si vous souhaitez que vos utilisateurs utilisent le protocole HTTPS et utilisent d'autres noms de domaine pour vos fichiers, choisissez l'une des options suivantes pour définir la manière dont les CloudFront requêtes HTTPS sont traitées :

- Utilisation de Server Name Indication (SNI) – recommandée
- Utilisez une adresse IP dédiée dans chaque emplacement périphérique

Cette section explique le mode de fonctionnement de chaque option.

Utilisation d’une extension SNI pour traiter les demandes HTTPS (fonctionne pour la plupart des clients)

Server Name Indication (SNI) est une extension du protocole TLS prise en charge par les navigateurs et les clients lancés après 2010. Si vous configurez CloudFront pour traiter les requêtes HTTPS à l'aide du SNI, CloudFront associez votre nom de domaine alternatif à une adresse IP pour chaque emplacement périphérique. Lorsqu’un utilisateur envoie une demande HTTPS pour votre contenu, DNS achemine la demande vers l’adresse IP de l’emplacement périphérique correct. L'adresse IP de votre nom de domaine est déterminée lors de la négociation de la SSL/TLS poignée de main ; l'adresse IP n'est pas dédiée à votre distribution.

La SSL/TLS négociation a lieu au début du processus d'établissement d'une connexion HTTPS. S'il n'est pas CloudFront possible de déterminer immédiatement à quel domaine concerne la demande, la connexion est interrompue. Lorsqu’une visionneuse prenant en charge SNI envoie une requête HTTPS pour obtenir votre contenu, voici ce qui se passe :

1. L’utilisateur récupère automatiquement le nom de domaine à partir de l’URL de la demande et l’ajoute à l’extension SNI du message TLS client hello.
2. Lorsqu'il CloudFront reçoit le client TLS hello, il utilise le nom de domaine dans l'extension SNI pour trouver la CloudFront distribution correspondante et renvoie le certificat TLS associé.
3. Le spectateur et la CloudFront SSL/TLS négociation sont effectués.
4. CloudFront renvoie le contenu demandé au visualiseur.

Pour une liste actuelle des navigateurs qui prennent en charge l’extension SNI, consultez l’entrée Server Name Indication de Wikipedia.

Si vous souhaitez utiliser l’extension SNI mais que certains navigateurs de vos utilisateurs ne la prennent pas en charge, vous disposez des solutions suivantes :

- Configurez CloudFront pour traiter les requêtes HTTPS en utilisant des adresses IP dédiées au lieu du SNI. Pour plus d’informations, consultez Utilisation d’une adresse IP dédiée pour traiter les demandes HTTPS (fonctionne pour tous les clients).
- Utilisez le CloudFront SSL/TLS certificat au lieu d'un certificat personnalisé. Cela nécessite que vous utilisiez le nom de CloudFront domaine de votre distribution dans les URL de vos fichiers, par exemple`https://d111111abcdef8.cloudfront.net/logo.png`.

Si vous utilisez le CloudFront certificat par défaut, les utilisateurs doivent prendre en charge le protocole SSL TLSv1 ou version ultérieure. CloudFront ne prend pas en charge le protocole SSLv3 avec le certificat par défautCloudFront .

Vous devez également modifier le SSL/TLS certificat que CloudFront vous utilisez, passant d'un certificat personnalisé à un CloudFront certificat par défaut :

- Si vous n'avez pas utilisé votre distribution pour transmettre votre contenu, vous pouvez juste modifier la configuration. Pour plus d'informations, consultez Mettre à jour une distribution.
- Si vous avez utilisé votre distribution pour diffuser votre contenu, vous devez créer une nouvelle CloudFront distribution et modifier les URL de vos fichiers afin de réduire ou d'éliminer la durée pendant laquelle votre contenu n'est pas disponible. Pour plus d'informations, consultez Revenir d'un SSL/TLS certificat personnalisé au certificat par défaut CloudFront.

- Si vous pouvez contrôler le navigateur employé par vos utilisateurs, demandez-leur de mettre leur navigateur à niveau afin qu'il accepte l'extension SNI.
- Utilisez HTTP au lieu de HTTPS.

Utilisation d'une adresse IP dédiée pour traiter les demandes HTTPS (fonctionne pour tous les clients)

L'utilisation d'une extension SNI (Server Name Indication) est une façon d'associer une demande à un domaine. Une autre méthode consiste à utiliser une adresse IP dédiée. Si vous avez des utilisateurs qui ne peuvent pas effectuer une mise à niveau vers un navigateur ou un client lancé après 2010, vous pouvez utiliser une adresse IP dédiée pour servir les demandes HTTPS. Pour une liste actuelle des navigateurs qui prennent en charge l'extension SNI, consultez l'entrée Server Name Indication de Wikipedia.

> **Important**
>
> Si vous configurez CloudFront pour traiter les requêtes HTTPS à l'aide d'adresses IP dédiées, des frais mensuels supplémentaires vous seront facturés. Les frais commencent lorsque vous associez votre SSL/TLS certificat à une distribution et que vous activez la distribution. Pour plus d'informations sur la CloudFront tarification, consultez la page CloudFront Tarification Amazon. Consultez également Using the Same Certificate for Multiple CloudFront Distributions.

Lorsque vous configurez CloudFront pour traiter les requêtes HTTPS à l'aide d'adresses IP dédiées, CloudFront associe votre certificat à une adresse IP dédiée dans chaque emplacement CloudFront périphérique. Lorsqu'une visionneuse envoie une requête HTTPS pour obtenir votre contenu, voici ce qui se passe :

1. DNS achemine la requête à l'adresse IP de votre distribution dans l'emplacement périphérique concerné.
2. Si une demande du client fournit l'extension SNI dans le `ClientHello` message, CloudFront recherche une distribution associée à ce SNI.
   - S'il y a une correspondance, CloudFront répond à la demande avec le SSL/TLS certificat.
   - S'il n'y a pas de correspondance, CloudFront utilise plutôt l'adresse IP pour identifier votre distribution et déterminer quel SSL/TLS certificat renvoyer à l'utilisateur.
3. CloudFront Visualisez et SSL/TLS négociez à l'aide de votre SSL/TLS certificat.
4. CloudFront renvoie le contenu demandé au visualiseur.

Cette méthode fonctionne pour toutes les requêtes HTTPS, quel que soit le navigateur ou autre client employé par l'utilisateur.

> **Note**
>
> Les adresses IP dédiées ne sont pas des adresses IP statiques et peuvent changer au fil du temps. L'adresse IP renvoyée pour l'emplacement périphérique est allouée dynamiquement à partir des plages d'adresses IP de la liste des serveurs CloudFront périphériques.
> Les plages d'adresses IP des serveurs CloudFront Edge sont susceptibles de changer.
> Pour être informé des changements d'adresse IP, abonnez-vous à AWS Public IP Address Changes en utilisant Amazon SNS.

Demandez l'autorisation d'utiliser au moins trois SSL/TLS certificats IP dédiés

Si vous avez besoin d'une autorisation pour associer de façon permanente au moins trois certificats IP SSL/TLS dédiés à CloudFront, effectuez la procédure suivante. Pour de plus amples informations sur les requêtes HTTPS, consultez Choisissez la manière dont CloudFront les requêtes HTTPS sont traitées.

> **Note**
>
> Cette procédure permet d'utiliser au moins trois certificats IP dédiés dans vos CloudFront distributions. La valeur par défaut est 2. N'oubliez pas que vous ne pouvez pas lier plusieurs certificats SSL à une distribution.
> Vous ne pouvez associer qu'un seul SSL/TLS certificat à une CloudFront distribution à la fois. Ce nombre correspond au nombre total de certificats IP SSL dédiés que vous pouvez utiliser dans toutes vos CloudFront distributions.

Pour demander l'autorisation d'utiliser trois certificats ou plus avec une CloudFront distribution

1. Accédez au Centre de support et créez une demande.
2. Indiquez le nombre de certificats dont vous avez besoin et décrivez les circonstances de votre demande. Votre compte sera mis à jour dès que possible.
3. Poursuivez avec la procédure suivante.

Exigences relatives à l'utilisation de SSL/TLS certificats avec CloudFront

Les exigences relatives aux SSL/TLS certificats sont décrites dans cette rubrique. Elles s'appliquent, sauf indication contraire, aux deux certificats suivants :

- Certificats pour l'utilisation du protocole HTTPS entre les spectateurs et CloudFront
- Certificats pour l'utilisation du protocole HTTPS entre CloudFront et votre point d'origine

Rubriques

- Auteur du certificat
- Région AWS for AWS Certificate Manager
- Format du certificat
- Certificats intermédiaires
- Type de clé
- Clé privée
- Permissions
- Taille de la clé de certificat

- Types de certificats pris en charge
- Date d'expiration de certificat et renouvellement
- Noms de domaine dans la CloudFront distribution et dans le certificat
- Version minimale SSL/TLS du protocole
- Versions de HTTP prises en charge

Auteur du certificat

Nous vous recommandons d'utiliser un certificat public délivré par AWS Certificate Manager (ACM). Pour plus d'informations sur l'obtention d'un certificat auprès d'ACM, reportez-vous au Guide de l'utilisateur AWS Certificate Manager. Pour utiliser un certificat ACM avec une CloudFront distribution, assurez-vous de demander (ou d'importer) le certificat dans la région USA Est (Virginie du Nord) (`us-east-1`).

CloudFront prend en charge les mêmes autorités de certification (CA) que Mozilla. Par conséquent, si vous n'utilisez pas ACM, utilisez un certificat émis par une autorité de certification figurant sur la liste des certificats CA inclus dans Mozilla.

Les certificats TLS utilisés par l'origine que vous avez spécifiée pour votre CloudFront distribution doivent également être émis par l'autorité de certification figurant sur la liste des certificats CA inclus dans Mozilla.

Pour plus de détails sur l'obtention et l'installation d'un certificat, consultez la documentation du logiciel de votre serveur HTTP et celle de l'autorité de certification.

Région AWS for AWS Certificate Manager

Pour utiliser un certificat dans AWS Certificate Manager (ACM) afin d'exiger le protocole HTTPS entre les utilisateursCloudFront, assurez-vous de demander (ou d'importer) le certificat dans la région USA Est (Virginie du Nord) (`us-east-1`).

Si vous souhaitez exiger le protocole HTTPS entre CloudFront et votre origine, et que vous utilisez un équilibreur de charge dans Elastic Load Balancing comme origine, vous pouvez demander ou importer le certificat dans n'importe quel Région AWS pays.

Format du certificat

Le certificat doit être au format X.509 PEM. Il s'agit du format par défaut si vous utilisez AWS Certificate Manager.

Certificats intermédiaires

Si vous utilisez une autorité de certification tierce, indiquez tous les certificats intermédiaires dans la chaîne de certificats du fichier `.pem`, en commençant par celui de l'autorité de certification qui a signé le certificat de votre domaine. En règle générale, vous trouverez sur le site web de votre autorité de certification un fichier répertoriant les certificats racines et intermédiaires dans l'ordre approprié pour la chaîne.

> **Important**
>
> N'incluez par les éléments suivants : le certificat racine, les certificats intermédiaires non approuvés ou le certificat de la clé publique de votre autorité de certification.

Voici un exemple :

```
-----BEGIN CERTIFICATE-----
Intermediate certificate 2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate certificate 1
-----END CERTIFICATE-----
```

Type de clé

CloudFront prend en charge les paires de clés publique-privée RSA et ECDSA.

CloudFront prend en charge les connexions HTTPS à la fois vers les spectateurs et les origines à l'aide de certificats RSA et ECDSA. Avec AWS Certificate Manager (ACM), vous pouvez demander et importer des certificats RSA ou ECDSA, puis les associer à votre distribution. CloudFront

Pour obtenir la liste des chiffrements RSA et ECDSA pris en charge par CloudFront ce protocole que vous pouvez négocier dans les connexions HTTPS, consultez et. the section called "Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront" the section called "Protocoles et chiffrements pris en charge entre CloudFront et l'origine"

Clé privée

Si vous utilisez un certificat d'une autorité de certification tierce, notez les points suivants :

- La clé privée doit correspondre à la clé publique qui se trouve dans le certificat.
- La clé privée doit être au format PEM.
- La clé privée ne peut pas être chiffrée avec un mot de passe.

Si AWS Certificate Manager (ACM) a fourni le certificat, ACM ne libère pas la clé privée. La clé privée est stockée dans ACM pour être utilisée par AWS les services intégrés à ACM.

Permissions

Vous devez être autorisé à utiliser et à importer le SSL/TLS certificat. Si vous utilisez AWS Certificate Manager (ACM), nous vous recommandons d'utiliser Gestion des identités et des accès AWS les autorisations pour restreindre l'accès aux certificats. Pour plus d'informations, consultez Gestion des identités et des accès dans le Guide de l'utilisateur AWS Certificate Manager .

Taille de la clé de certificat

La taille de clé de certificat CloudFront prise en charge dépend du type de clé et de certificat.

Pour les certificats RSA :

CloudFront prend en charge les clés RSA 1024 bits, 2048 bits, 3072 bits et 4096 bits. La longueur de clé maximale pour un certificat RSA que vous utilisez CloudFront est de 4 096 bits.

Notez qu'ACM émet des certificats RSA avec des clés limitées à 2 048 bits. Pour utiliser un certificat RSA 3072 bits ou 4096 bits, vous devez obtenir le certificat en externe et l'importer dans ACM, après quoi vous pourrez l'utiliser. CloudFront

Pour en savoir plus sur la façon de déterminer la taille d'une clé RSA, consultez Déterminer la taille de la clé publique dans un certificat SSL/TLS RSA.

Pour les certificats ECDSA :

CloudFront prend en charge les clés 256 bits et 384 bits. Pour utiliser un certificat ECDSA dans ACM afin d'exiger le protocole HTTPS entre les spectateurs etCloudFront, utilisez la courbe elliptique prime256v1 ou secp384r1.

Types de certificats pris en charge

CloudFront prend en charge tous les types de certificats émis par une autorité de certification fiable.

Date d’expiration de certificat et renouvellement

Si vous utilisez des certificats obtenus auprès d'une autorité de certification (CA) tierce, vous devez surveiller les dates d'expiration des certificats et renouveler les certificats que vous importez dans AWS Certificate Manager (ACM) ou que vous téléchargez dans le magasin de Gestion des identités et des accès AWS certificats avant leur expiration.

> **Important**
>
> Pour éviter les problèmes liés à l’expiration d’un certificat, renouvelez ou réimportez votre certificat au moins 24 heures avant la valeur `NotAfter` de votre certificat actuel. Si votre certificat expire dans les 24 heures, demandez un nouveau certificat à ACM ou importez-en un nouveau dans ACM. Associez ensuite le nouveau certificat à la CloudFront distribution. CloudFront peut continuer à utiliser le certificat précédent pendant que le renouvellement ou la réimportation de votre certificat est en cours. Il s'agit d'un processus asynchrone qui peut prendre jusqu'à 24 heures avant que vos modifications ne CloudFront soient affichées.

Si vous utilisez des certificats fournis par ACM, ACM gère automatiquement le renouvellement des certificats. Pour plus d'informations, consultez Renouvellement géré dans le Guide de l'utilisateur AWS Certificate Manager .

Noms de domaine dans la CloudFront distribution et dans le certificat

Lorsque vous utilisez une origine personnalisée, le SSL/TLS certificat correspondant à votre origine inclut un nom de domaine dans le champ Nom commun, et éventuellement plusieurs autres dans le champ Subject Alternative Names. (CloudFront prend en charge les caractères génériques dans les noms de domaine des certificats.)

L’un des noms de domaines du certificat doit correspondre au nom de domaine spécifié pour le nom du domaine d’origine. Si aucun nom de domaine ne correspond, CloudFront renvoie le code d'état HTTP `502 (Bad Gateway)` au visualiseur.

> **Important**
>
> Lorsque vous ajoutez un autre nom de domaine à une distribution, CloudFront vérifie que ce nom de domaine alternatif est couvert par le certificat que vous avez joint. Le certificat doit couvrir le nom de domaine alternatif dans le champ SAN du certificat. Cela signifie que le

champ SAN doit contenir une correspondance exacte pour le nom de domaine alternatif ou un caractère générique au même niveau que le nom de domaine alternatif que vous ajoutez. Pour plus d'informations, consultez Exigences relatives à l'utilisation de noms de domaines alternatifs.

Version minimale SSL/TLS du protocole

Si vous utilisez des adresses IP dédiées, définissez la version minimale du SSL/TLS protocole pour la connexion entre les spectateurs et CloudFront en choisissant une politique de sécurité.

Pour plus d'informations, consultez Politique de sécurité (SSL/TLS version minimale) dans la rubrique Référence de tous les paramètres de distribution.

Versions de HTTP prises en charge

Si vous associez un certificat à plusieurs CloudFront distributions, toutes les distributions associées au certificat doivent utiliser la même option pourVersions de HTTP prises en charge. Vous spécifiez cette option lorsque vous créez ou mettez à jour une CloudFront distribution.

Quotas d'utilisation de SSL/TLS certificats avec CloudFront (HTTPS entre spectateurs et CloudFront uniquement)

Prenez note des quotas suivants concernant l'utilisation de SSL/TLS certificats avecCloudFront. Ces quotas s'appliquent uniquement aux SSL/TLS certificats que vous approvisionnez à l'aide de AWS Certificate Manager (ACM), que vous importez dans ACM ou que vous téléchargez vers le magasin de certificats IAM pour les communications HTTPS entre les utilisateurs et. CloudFront

Pour plus d'informations, consultez Augmenter les quotas de SSL/TLS certificats.

Nombre maximum de certificats par CloudFront distribution

Vous pouvez associer au maximum un SSL/TLS certificat à chaque CloudFront distribution.

Nombre maximal de certificats que vous pouvez importer dans ACM ou télécharger dans le magasin de certificats IAM

Si vous avez obtenu vos SSL/TLS certificats auprès d'une autorité de certification tierce, vous devez les stocker dans l'un des emplacements suivants :

- AWS Certificate Manager – Pour connaître le quota actuel sur le nombre de certificats ACM, consultez Quotas dans le Guide de l'utilisateur AWS Certificate Manager . Le quota indiquée est

un total qui inclut les certificats que vous mettez en service à l'aide d'ACM et les certificats que vous importez dans ACM.

- Magasin de certificats IAM : pour connaître le quota actuel (anciennement appelé limite) du nombre de certificats que vous pouvez télécharger dans le magasin de certificats IAM pour un AWS compte, consultez la section Limites IAM et STS dans le guide de l'utilisateur IAM. Vous pouvez demander une augmentation de quota dans la console Service Quotas.

Nombre maximum de certificats par AWS compte (adresses IP dédiées uniquement)

Si vous souhaitez diffuser des requêtes HTTPS en utilisant des adresses IP dédiées, notez les points suivants :

- Par défaut, vous CloudFront autorise à utiliser deux certificats avec votre AWS compte, l'un pour un usage quotidien et l'autre lorsque vous devez alterner les certificats pour plusieurs distributions.
- Si vous avez besoin de plus de deux SSL/TLS certificats personnalisés pour votre AWS compte, vous pouvez demander un quota plus élevé dans la console Service Quotas.

Utilisez le même certificat pour les CloudFront distributions créées à l'aide de différents AWS comptes

Si vous utilisez une autorité de certification tierce et que vous souhaitez utiliser le même certificat avec plusieurs CloudFront distributions créées à l'aide de différents AWS comptes, vous devez importer le certificat dans ACM ou le télécharger dans le magasin de certificats IAM une fois pour chaque AWS compte.

Si vous utilisez des certificats fournis par ACM, vous ne pouvez pas configurer CloudFront pour utiliser des certificats créés par un autre AWS compte.

Utilisez le même certificat pour CloudFront et pour les autres AWS services

Si vous avez acheté un certificat auprès d'une autorité de certification fiable telle que Comodo ou Symantec, vous pouvez utiliser le même certificat pour CloudFront et pour d'autres services. DigiCert AWS Si vous importez le certificat dans ACM, vous ne devez l'importer qu'une seule fois pour l'utiliser pour plusieurs services AWS .

Si vous utilisez les certificats fournis par ACM, ces certificats sont stockés dans ACM.

Utiliser le même certificat pour plusieurs CloudFront distributions

Vous pouvez utiliser le même certificat pour tout ou partie des distributions CloudFront que vous utilisez pour diffuser les requêtes HTTPS. Notez ce qui suit :

- Vous pouvez utiliser le même certificat pour diffuser les requêtes utilisant des adresses IP dédiées et pour celles utilisant l’extension SNI.
- Vous ne pouvez associer qu’un seul certificat à chaque distribution.
- Chaque distribution doit inclure un ou plusieurs noms de domaines alternatifs qui apparaissent aussi dans les champs Common Name ou Subject Alternative Name du certificat.
- Si vous envoyez des requêtes HTTPS à l'aide d'adresses IP dédiées et que vous avez créé toutes vos distributions à l'aide du même AWS compte, vous pouvez réduire considérablement vos coûts en utilisant le même certificat pour toutes les distributions. CloudFront des frais pour chaque certificat, et non pour chaque distribution.

  Supposons, par exemple, que vous créiez trois distributions à l'aide du même AWS compte et que vous utilisiez le même certificat pour les trois distributions. Un seul montant correspondant à l’usage des adresses IP dédiées vous sera facturé.

  Toutefois, si vous envoyez des requêtes HTTPS à l'aide d'adresses IP dédiées et que vous utilisez le même certificat pour créer des CloudFront distributions sur différents AWS comptes, les frais d'utilisation d'adresses IP dédiées sont facturés à chaque compte. Par exemple, si vous créez trois distributions à l'aide de trois AWS comptes différents et que vous utilisez le même certificat pour les trois distributions, chaque compte est facturé intégralement pour l'utilisation d'adresses IP dédiées.

Configuration de noms de domaines alternatifs et HTTPS

Pour utiliser des noms de domaine alternatifs dans les URL de vos fichiers et pour utiliser le protocole HTTPS entre les utilisateurs CloudFront, effectuez les procédures applicables.

Rubriques

- Obtenir un SSL/TLS certificat
- Importer un SSL/TLS certificat
- Mettez à jour votre CloudFront distribution

Obtenir un SSL/TLS certificat

Procurez-vous un SSL/TLS certificat si vous n'en avez pas déjà un. Pour plus d'informations, consultez la documentation pertinente :

- Pour utiliser un certificat fourni par AWS Certificate Manager (ACM), consultez le Guide de l'AWS Certificate Manager utilisateur. Passez ensuite à Mettez à jour votre CloudFront distribution.

> **Note**
>
> Nous vous recommandons d'utiliser ACM pour provisionner, gérer et déployer des SSL/TLS certificats sur des ressources AWS gérées. Vous devez demander un certificat ACM dans la région USA Est (Virginie du Nord).

- Pour obtenir un certificat auprès d'une autorité de certification tierce, consultez la documentation fournie par l'autorité de certification. Lorsque vous avez obtenu le certificat, passez à la procédure suivante.

Importer un SSL/TLS certificat

Si vous avez obtenu votre certificat auprès d'une autorité de certification tierce, importez-le dans ACM ou chargez-le dans le magasin de certificats IAM :

ACM (recommandé)

Avec ACM, vous pouvez importer des certificats tiers depuis la console ACM, ainsi que par programmation. Pour plus d'informations sur l'importation d'un certificat dans ACM, consultez Importation de certificats dans AWS Certificate Manager dans le Guide de l'utilisateur AWS Certificate Manager . Vous devez importer le certificat dans la région USA Est (Virginie du Nord).

Magasin de certificats IAM

(Non recommandé) Utilisez la AWS CLI commande suivante pour télécharger votre certificat tiers dans le magasin de certificats IAM.

```
aws iam upload-server-certificate \
        --server-certificate-name CertificateName \
        --certificate-body file://public_key_certificate_file \
        --private-key file://privatekey.pem \
        --certificate-chain file://certificate_chain_file \
        --path /cloudfront/path/
```

Notez ce qui suit :

- AWS compte : vous devez télécharger le certificat dans le magasin de certificats IAM en utilisant le même AWS compte que celui que vous avez utilisé pour créer votre CloudFront distribution.
- Paramètre --path : lorsque vous chargez le certificat dans IAM, la valeur du paramètre `--path` (chemin du certificat) doit commencer par `/cloudfront/`, comme `/cloudfront/production/` ou `/cloudfront/test/`. Le chemin doit se terminer par un caractère /.
- Certificats existants : vous devez affecter aux paramètres `--server-certificate-name` et `--path` des valeurs différentes de celles qui sont associées aux certificats existants.
- Utilisation de la CloudFront console : la valeur que vous spécifiez pour le `--server-certificate-name` paramètre dans AWS CLI, par exemple`mySServerCertificate`, apparaît dans la liste des certificats SSL de la CloudFront console.
- Utilisation de l' CloudFront API : notez la chaîne alphanumérique AWS CLI renvoyée, `AS1A2M3P4L5E67SIIXR3J` par exemple. Il s'agit de la valeur que vous spécifierez dans l'élément `IAMCertificateId`. Vous n'avez pas besoin de l'ARN IAM, que renvoie également la CLI.

Pour plus d'informations à ce sujet AWS CLI, consultez le Guide de AWS Command Line Interface l'utilisateur et la Référence des AWS CLI commandes.

Mettez à jour votre CloudFront distribution

Pour mettre à jour les paramètres de votre distribution, procédez comme suit :

Pour configurer votre CloudFront distribution pour les noms de domaine alternatifs

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution que vous souhaitez mettre à jour.
3. Sous l'onglet General, choisissez Edit.
4. Mettez à jour les valeurs suivantes :

   Nom de domaine alternatif (CNAME)

   Choisissez Ajouter un élément pour ajouter les noms de domaine alternatifs applicables. Séparez les noms de domaines par des virgules ou saisissez chaque nom de domaine sur une nouvelle ligne.

Certificat SSL personnalisé

Sélectionnez un certificat dans la liste déroulante.

Jusqu'à 100 certificats sont répertoriés ici. Si vous avez plus de 100 certificats et que vous ne voyez pas le certificat que vous souhaitez ajouter, vous pouvez taper un nom ARN de certificat dans le champ pour le choisir.

Si vous avez chargé un certificat dans le magasin de certificats IAM mais qu'il n'apparaît pas dans la liste et que vous ne pouvez pas le choisir en tapant son nom dans le champ, revoyez la procédure Importer un SSL/TLS certificat afin de vérifier si vous avez bien chargé le certificat.

> **Important**
>
> Après avoir associé votre SSL/TLS certificat à votre CloudFront distribution, ne supprimez pas le certificat d'ACM ou du magasin de certificats IAM tant que vous n'avez pas supprimé le certificat de toutes les distributions et que toutes les distributions n'ont pas été déployées.

5. Cliquez sur Enregistrer les modifications.
6. Configurez CloudFront pour exiger le protocole HTTPS entre les spectateurs et CloudFront :

   a. Sous l'onglet Comportements, choisissez le comportement de cache à mettre à jour, puis sélectionnez Modifier.

   b. Spécifiez l'une des valeurs suivantes pour Politique de protocole d'utilisateur :

      Redirect HTTP to HTTPS

      Les utilisateurs peuvent utiliser les deux protocoles, mais les requêtes HTTP sont automatiquement redirigées vers les requêtes HTTPS. CloudFront renvoie le code d'état HTTP `301 (Moved Permanently)`, ainsi que la nouvelle URL HTTPS. L'utilisateur soumet ensuite à nouveau la demande à CloudFront l'aide de l'URL HTTPS.

      > **Important**
      >
      > CloudFront ne redirige pas `DELETEOPTIONS`, `PATCHPOST`, ou les `PUT` requêtes de HTTP vers HTTPS. Si vous configurez un comportement de cache pour rediriger vers HTTPS, CloudFront répondez à `HTTPDELETE,OPTIONS`,

PATCHPOST, ou à des PUT demandes concernant ce comportement de cache avec un code d'état HTTP403 (Forbidden).

Lorsqu'un utilisateur effectue une requête HTTP qui est redirigée vers une requête HTTPS, CloudFront les deux demandes sont facturées. Pour la requête HTTP, le montant correspond uniquement à la requête et aux en-têtes que CloudFront renvoie à l'utilisateur. Pour la requête HTTPS, le montant correspond à la requête ainsi qu'aux en-têtes et au fichier renvoyés par votre origine.

HTTPS Only

Les visionneuses ne peuvent accéder au contenu que si elles utilisent le protocole HTTPS. Si un utilisateur envoie une requête HTTP au lieu d'une requête HTTPS, il CloudFront renvoie le code 403 (Forbidden) d'état HTTP mais ne renvoie pas le fichier.

c. Choisissez Oui, Modifier.

d. Répétez les étapes a à c pour chaque comportement de cache supplémentaire pour lequel vous souhaitez exiger HTTPS entre les visionneuses et CloudFront.

7. Vérifiez les éléments suivants avant d'utiliser la configuration mise à jour dans un environnement de production :

- Le modèle de chemin de chaque comportement de cache s'applique uniquement aux requêtes pour lesquelles vous souhaitez que les visionneuses utilisent HTTPS.
- Les comportements de cache sont répertoriés dans l'ordre dans lequel vous voulez que CloudFront les évalue. Pour plus d'informations, consultez Modèle de chemin.
- Les comportements de cache acheminent les requêtes vers les origines correctes.

Déterminer la taille de la clé publique dans un certificat SSL/TLS RSA

Lorsque vous utilisez des noms de domaine CloudFront alternatifs et HTTPS, la taille maximale de la clé publique dans un certificat SSL/TLS RSA est de 4 096 bits. (Il s'agit de la taille de la clé, et non pas du nombre de caractères figurant dans la clé publique.) Si vous utilisez AWS Certificate Manager pour vos certificats, bien qu'ACM prenne en charge des clés RSA plus grandes, vous ne pouvez pas utiliser les clés plus grandes avec. CloudFront

Vous pouvez déterminer la taille de la clé publique RSA en exécutant la commande OpenSSL suivante :

```
openssl x509 -in path and filename of SSL/TLS certificate -text -noout
```

Où :

- `-in` spécifie le chemin et le nom de fichier de votre certificat SSL/TLS RSA.
- `-text` permet à OpenSSL d'afficher la longueur de la clé publique RSA en bits.
- `-noout` empêche OpenSSL d'afficher la clé publique.

Exemple de sortie :

```
Public-Key: (2048 bit)
```

Augmenter les quotas de SSL/TLS certificats

Il existe des quotas quant au nombre de SSL/TLS certificats que vous pouvez importer dans AWS Certificate Manager (ACM) ou télécharger vers Gestion des identités et des accès AWS (IAM). Il existe également un quota sur le nombre de SSL/TLS certificats que vous pouvez utiliser avec et Compte AWS lorsque vous configurez CloudFront pour traiter les requêtes HTTPS à l'aide d'adresses IP dédiées. Cependant, vous pouvez demander des quotas plus élevés.

Rubriques

- Augmentation du quota de certificats importés dans ACM
- Augmentation du quota de certificats téléchargés vers IAM
- Augmentation du quota de certificats utilisés avec des adresses IP dédiées

Augmentation du quota de certificats importés dans ACM

Pour connaître le quota du nombre de certificats que vous pouvez importer dans ACM, consultez la page Quotas dans le Guide de l'utilisateur AWS Certificate Manager .

Pour demander l'augmentation d'un quota, utilisez la console Service Quotas. Pour plus d'informations, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Augmentation du quota de certificats téléchargés vers IAM

Pour connaître le quota (auparavant appelé limite) lié au nombre de certificats que vous pouvez charger dans IAM, consultez Limites IAM et STS dans le Guide de l'utilisateur IAM.

Pour demander l'augmentation d'un quota, utilisez la console Service Quotas. Pour plus d'informations, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Augmentation du quota de certificats utilisés avec des adresses IP dédiées

Pour connaître le quota de certificats SSL que vous pouvez utiliser pour chacun d'eux Compte AWS lorsque vous répondez à des requêtes HTTPS à l'aide d'adresses IP dédiées, consultezQuotas sur les certificats SSL.

Pour demander l'augmentation d'un quota, utilisez la console Service Quotas. Pour plus d'informations, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Rotation SSL/TLS des certificats

Lorsque vos SSL/TLS certificats arrivent à expiration, vous devez les alterner pour garantir la sécurité de votre distribution et éviter toute interruption de service pour vos spectateurs. Vous pouvez effectuer leur rotation selon les méthodes suivantes :

- Pour les SSL/TLS certificats fournis par AWS Certificate Manager (ACM), il n'est pas nécessaire de les alterner. ACM gère automatiquement le renouvellement des certificats. Pour plus d'informations, consultez Renouvellement géré des certificats dans le Guide de l'utilisateur AWS Certificate Manager .
- Si vous utilisez une autorité de certification tierce et que vous avez importé des certificats dans ACM (recommandé) ou que vous en avez chargé dans le magasin de certificats IAM, vous devez parfois remplacer un certificat par un autre.

> **Important**
>
> - ACM ne gère pas le renouvellement des certificats que vous obtenez auprès d'autorités de certification tierces et importez dans ACM.

- Si vous avez configuré CloudFront pour traiter les requêtes HTTPS à l'aide d'adresses IP dédiées, l'utilisation d'un ou de plusieurs certificats supplémentaires lors de la rotation des certificats peut entraîner des frais supplémentaires calculés au prorata. Nous vous recommandons de mettre à jour vos distributions pour réduire les frais supplémentaires.

Rotation SSL/TLS des certificats

Pour faire tourner vos certificats, exécutez la procédure suivante. Les utilisateurs peuvent continuer d'accéder à votre contenu pendant la rotation des certificats, ainsi qu'une fois le processus terminé.

Pour alterner SSL/TLS les certificats

1. Augmenter les quotas de SSL/TLS certificats pour déterminer si vous avez besoin de l'autorisation d'utiliser Plus de certificats SSL. Si c'est le cas, demandez l'autorisation et attendez que celle-ci vous soit accordée avant de passer à l'étape 2.
2. Importez le nouveau certificat dans ACM ou chargez-le dans IAM. Pour plus d'informations, consultez la section Importation d'un SSL/TLS certificat dans l'Amazon CloudFront Developer Guide.
3. (Pour les certificats IAM uniquement) Mettez vos distributions à jour une à la fois pour utiliser le nouveau certificat. Pour plus d'informations, consultez Mettre à jour une distribution.
4. (Facultatif) Supprimez le certificat précédent d'ACM ou d'IAM.

> **Important**
>
> Ne supprimez pas un SSL/TLS certificat tant que vous ne l'avez pas supprimé de toutes les distributions et que le statut des distributions que vous avez mises à jour n'est pas passé à`Deployed`.

Revenir d'un SSL/TLS certificat personnalisé au certificat par défaut CloudFront

Si vous avez configuré CloudFront pour utiliser le protocole HTTPS entre les spectateurs et CloudFront et que vous avez configuré CloudFront pour utiliser un SSL/TLS certificat personnalisé, vous pouvez modifier votre configuration pour utiliser le CloudFront SSL/TLS certificat par défaut. Le processus varie selon que vous avez utilisé ou non votre distribution pour transmettre votre contenu :

- Si vous n’avez pas utilisé votre distribution pour transmettre votre contenu, vous pouvez juste modifier la configuration. Pour plus d’informations, consultez Mettre à jour une distribution.
- Si vous avez utilisé la distribution pour transmettre votre contenu, vous devez créer une nouvelle distribution CloudFront et modifier les URL de fichiers afin de réduire ou d'éliminer la durée d'indisponibilité de votre contenu. Pour ce faire, procédez comme suit.

Revenir au certificat par défaut CloudFront

La procédure suivante vous montre comment revenir d'un SSL/TLS certificat personnalisé au CloudFront certificat par défaut.

Pour revenir au certificat par défaut CloudFront

1. Créez une nouvelle CloudFront distribution avec la configuration souhaitée. Pour Certificat SSL, choisissez Certificat par défaut CloudFront (*.cloudfront.net).

   Pour plus d’informations, consultez Créer une distribution.
2. Pour les fichiers que vous utilisez pour distribuer CloudFront, mettez à jour les URL de votre application afin d'utiliser le nom de domaine CloudFront attribué à la nouvelle distribution. Remplacez, par exemple, `https://www.example.com/images/logo.png` par `https://d111111abcdef8.cloudfront.net/images/logo.png`.
3. Supprimez la distribution associée à un SSL/TLS certificat personnalisé ou mettez-la à jour pour changer la valeur du certificat SSL en CloudFront certificat par défaut (*.cloudfront.net). Pour plus d’informations, consultez Mettre à jour une distribution.

   > **Important**
   >
   > Jusqu'à ce que vous ayez terminé cette étape, AWS continue de vous facturer pour l'utilisation d'un SSL/TLS certificat personnalisé.

4. (Facultatif) Supprimez votre SSL/TLS certificat personnalisé.

   a. Exécutez la AWS CLI commande `list-server-certificates` pour obtenir l'ID du certificat que vous souhaitez supprimer. Pour plus d’informations, consultez list-server-certificates dans la Référence des commandes AWS CLI .

b. Exécutez la AWS CLI commande `delete-server-certificate` pour supprimer le certificat. Pour plus d'informations, consultez delete-server-certificate dans la Référence des commandes AWS CLI .

Passez d'un SSL/TLS certificat personnalisé avec des adresses IP dédiées au SNI

Si vous avez configuré CloudFront pour utiliser un SSL/TLS certificat personnalisé avec des adresses IP dédiées, vous pouvez passer à l'utilisation d'un SSL/TLS certificat personnalisé avec SNI à la place et éliminer les frais associés aux adresses IP dédiées.

> **Important**
>
> Cette mise à jour de votre CloudFront configuration n'a aucun effet sur les utilisateurs qui prennent en charge le SNI. Les spectateurs peuvent accéder à votre contenu avant et après la modification, ainsi que pendant que celle-ci se propage vers les zones CloudFront périphériques. Les utilisateurs qui ne prennent pas en charge l'extension SNI ne peuvent plus accéder à votre contenu après le changement. Pour plus d'informations, consultez Choisissez la manière dont CloudFront les requêtes HTTPS sont traitées.

Conversion d'un certificat personnalisé à une extension SNI

La procédure suivante explique comment passer d'un SSL/TLS certificat personnalisé avec des adresses IP dédiées à un certificat SNI.

Pour passer d'un SSL/TLS certificat personnalisé avec des adresses IP dédiées à un certificat SNI

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution que vous souhaitez afficher ou mettre à jour.
3. Choisissez Paramètres de distribution.
4. Sous l'onglet General, choisissez Edit.
5. Dans Certification SSL personnalisée – facultatif, désélectionnez Prise en charge de clients hérités.
6. Choisissez Oui, Modifier.

Authentification TLS mutuelle avec CloudFront (Viewer MTLS)

L'authentification TLS mutuelle (Mutual Transport Layer Security Authentication — MTLS) est un protocole de sécurité qui étend l'authentification TLS standard en exigeant une authentification bidirectionnelle basée sur des certificats, dans laquelle le client et le serveur doivent prouver leur identité avant d'établir une connexion sécurisée. Grâce au protocole TLS mutuel, vous pouvez vous assurer que seuls les clients présentant des certificats TLS fiables ont accès à vos CloudFront distributions.

Comment ça marche

Dans un handshake TLS standard, seul le serveur présente un certificat prouvant son identité au client. Avec le protocole TLS mutuel, le processus d'authentification devient bidirectionnel. Lorsqu'un client tente de se connecter à votre CloudFront distribution, il CloudFront demande un certificat client lors de la prise de contact TLS. Le client doit présenter un X.509 certificat valide par rapport à votre magasin de confiance configuré avant d'établir la connexion sécurisée. CloudFront

CloudFront effectue cette validation des certificats sur des sites AWS périphériques, déchargeant ainsi vos serveurs d'origine de la complexité de l'authentification tout en préservant les avantages en termes de performances à l' CloudFront échelle mondiale. Vous pouvez configurer les MTLs selon trois modes :

- Mode obligatoire (par défaut) : CloudFront valide le certificat client par rapport à un magasin de confiance. Si la validation échoue ou si aucun certificat n'est présenté, CloudFront refuse la connexion. Utilisez le mode obligatoire lorsque chaque client doit s'authentifier avec un certificat valide.
- Mode facultatif : CloudFront valide le certificat client s'il est présenté, mais autorise les connexions sans certificat. Les métadonnées du certificat sont disponibles dans les fonctions de connexion et les en-têtes HTTP pour que votre origine prenne des décisions d'autorisation. Utilisez le mode facultatif lorsque vous prenez en charge les clients authentifiés et non authentifiés.
- Mode passthrough : CloudFront ne valide pas le certificat client par rapport à un magasin de confiance. CloudFront valide uniquement que le client possède la clé privée correspondante. Il transmet le certificat à votre origine sous forme d'en-têtes HTTP permettant à votre origine d'effectuer la validation. Aucun magasin de confiance n'est requis et aucune mise en cache n'a lieu. Utilisez le mode passthrough lorsque vous avez des implémentations MTLS existantes à votre origine.

Pour plus d'informations sur ces modes de validation, consultezModes de validation supplémentaires.

Cas d’utilisation

L'authentification TLS mutuelle CloudFront répond à plusieurs scénarios de sécurité critiques dans lesquels les méthodes d'authentification traditionnelles sont insuffisantes :

- Authentification des appareils avec mise en cache du contenu : vous pouvez authentifier les consoles de jeu, les appareils IoT ou le matériel de l'entreprise avant d'autoriser l'accès aux mises à jour du microprogramme, aux téléchargements de jeux ou aux ressources internes. Chaque appareil contient un certificat unique qui prouve son authenticité tout en bénéficiant des fonctionnalités de CloudFront mise en cache.
- API-to-API authentification - Vous pouvez sécuriser les communications de machine à machine entre des partenaires commerciaux de confiance, des systèmes de paiement ou des microservices. Certificate-based l'authentification élimine le besoin de partager des secrets ou des clés d'API tout en fournissant une solide vérification d'identité pour les échanges de données automatisés.

Rubriques

- Trust Stores et gestion des certificats
- Activer le protocole TLS mutuel pour les distributions CloudFront
- Associer une fonction CloudFront de connexion
- Configuration de paramètres supplémentaires
- En-têtes MTLS Viewer pour les politiques de cache et transférés à l'origine
- Révocation du certificat
- Méthodes auxiliaires pour le protocole TLS mutuel
- Modes de validation supplémentaires
- Observabilité à l'aide des journaux de connexion

Trust Stores et gestion des certificats

La création et la configuration d'un trust store sont obligatoires pour implémenter l'authentification TLS mutuelle avec CloudFront. Les magasins de confiance contiennent les certificats de l'autorité de certification (CA) CloudFront utilisés pour valider les certificats clients lors du processus d'authentification.

Qu'est-ce qu'un trust store ?

Un trust store est un référentiel de certificats CA CloudFront utilisé pour valider les certificats clients lors de l'authentification TLS mutuelle. Les magasins de confiance contiennent les certificats racine et intermédiaires de l'autorité de certification qui forment la chaîne de confiance pour authentifier les certificats clients.

Lorsque vous implémentez le protocole TLS mutuel avec CloudFront, le trust store définit les autorités de certification auxquelles vous faites confiance pour délivrer des certificats clients valides. CloudFront valide chaque certificat client par rapport à votre magasin de confiance lors de la prise de contact TLS. Seuls les clients présentant des certificats liés à l'une des autorités de certification de votre trust store seront authentifiés avec succès.

Les dépôts de confiance CloudFront sont des ressources au niveau du compte que vous pouvez associer à plusieurs distributions. Vous pouvez ainsi maintenir des politiques de validation des certificats cohérentes tout au long de votre CloudFront déploiement tout en simplifiant la gestion des certificats CA.

Assistance aux autorités de certification

CloudFront prend en charge les certificats émis à la fois par une autorité de certification AWS privée et par des autorités de certification privées tierces. Grâce à cette flexibilité, vous pouvez utiliser votre infrastructure de certificats existante ou tirer parti des services de certificats AWS gérés en fonction des besoins de votre organisation.

- AWS Autorité de certification privée : vous pouvez utiliser des certificats émis par AWS Private CA, qui fournit un service d'autorité de certification privée géré. Cette intégration simplifie la gestion du cycle de vie des certificats et permet une intégration parfaite avec d'autres AWS services.
- Third-party Autorités de certification privées : vous pouvez également utiliser des certificats provenant de votre infrastructure d'autorité de certification privée existante, y compris des autorités de certification d'entreprise ou d'autres fournisseurs de certificats tiers. Vous pouvez ainsi maintenir vos processus actuels de gestion des certificats tout en ajoutant des fonctionnalités CloudFront MTL.

Exigences et spécifications relatives aux certificats

Les magasins de confiance ont des exigences spécifiques concernant les certificats CA qu'ils contiennent :

Exigences relatives au format des certificats CA

- Format : format PEM (Privacy Enhanced Mail)
- Limites du contenu : les certificats doivent être placés dans les limites -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----
- Commentaires : Doit être précédé d'un caractère # et ne peut contenir aucun caractère -
- Sauts de ligne : aucune ligne vide n'est autorisée entre les certificats

Spécifications des certificats pris en charge

- Type de certificat : X.509v3
- Types de clés publiques :
  - RSA 2048, RSA 3072, RSA 4096
  - ECDSA : secp256r1, secp384r1, secp521r1
- Algorithmes de signature :
  - SHA256, SHA384, SHA512 avec RSA
  - SHA256, SHA384, SHA512 avec EC
  - SHA256, SHA384, SHA512 avec MGF1 RSASSA-PSS

Exemple de format de bundle de certificats

Certificats multiples (PEM-encoded) :

```
# Root CA Certificate
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIJAKoK/OvD/XqiMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNzEyMTU0NzQ4WhcNMjcwNzEwMTU0NzQ4WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuuExKvY1xzHFylsHiuowqpmzs7rEcuuylOuEszpFp+BtXh0ZuEtts9LP
-----END CERTIFICATE-----
# Intermediate CA Certificate
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIJAKoK/OvD/XqjMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQwHhcNMTcwNzEyMTU0NzQ4WhcNMjcwNzEwMTU0NzQ4WjBF
MQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50
```

```
ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuuExKvY1xzHFylsHiuowqpmzs7rEcuuylOuEszpFp+BtXh0ZuEtts9LP
-----END CERTIFICATE-----
```

Créez un trust store

Avant de créer un trust store, vous devez télécharger votre bundle de certificats CA au format PEM dans un compartiment Amazon S3. Le bundle de certificats doit contenir tous les certificats d'autorité de certification racine et intermédiaire sécurisés nécessaires à la validation de vos certificats clients.

Le bundle de certificats CA n'est lu qu'une seule fois depuis S3 lors de la création d'un trust store. Si de futures modifications sont apportées au bundle de certificats CA, le trust store devra être mis à jour manuellement. Aucune synchronisation n'est maintenue entre le trust store et le bundle de certificats S3 CA.

Conditions préalables

- Un bundle de certificats de votre autorité de certification (CA) chargé dans un compartiment Amazon S3
- Les autorisations nécessaires pour créer des CloudFront ressources

Pour créer un trust store (console)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Trust stores.
3. Choisissez Create trust store.
4. Dans Nom de la boutique de confiance, entrez le nom de votre boutique de confiance.
5. Pour le bundle d'autorité de certification (CA), entrez le chemin Amazon S3 vers votre bundle de certificats PEM-format CA.
6. Choisissez Create trust store.

Pour créer un magasin de confiance (AWS CLI)

```
aws cloudfront create-trust-store \
  --name MyTrustStore \
  --ca-certificates-bundle-source '{"CaCertificatesBundleS3Location":{"Bucket":"my-
bucket","Key":"ca-bundle.pem","Region":"bucket-region"}}' \
```

```
  --tags Items=[{Key=Environment,Value=Production}]
```

Associez Trust Store aux distributions

Après avoir créé un trust store, vous devez l'associer à une CloudFront distribution pour permettre l'authentification TLS mutuelle.

Conditions préalables

- Une CloudFront distribution existante avec la politique de protocole de HTTPS-only visualisation activée et le support HTTP3 désactivé.

Pour associer un trust store (console)

Il existe deux manières d'associer un trust store dans la CloudFront console : via la page de détails du trust store ou via la page des paramètres de distribution.

Associer un trust store via la page de détails du trust store :

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Trust stores.
3. Choisissez le nom du trust store que vous souhaitez associer.
4. Choisissez Associer à la distribution.
5. Configurez les options mTLS du Viewer disponibles :

    - Mode de validation du certificat client : choisissez entre le mode obligatoire et le mode facultatif. En mode obligatoire, tous les clients sont tenus de présenter des certificats. En mode facultatif, les clients qui présentent des certificats sont validés, tandis que les clients qui ne présentent pas de certificats sont autorisés à y accéder.
    - Publiez les noms des autorités de certification de confiance : choisissez si vous souhaitez annoncer les noms des autorités de certification de votre boutique de confiance aux clients lors de la poignée de main TLS.
    - Ignorer la date d'expiration du certificat : choisissez si vous souhaitez autoriser les connexions avec des certificats expirés (les autres critères de validation s'appliquent toujours).
    - Fonction de connexion : une fonction de connexion optionnelle peut être associée aux allow/deny connexions en fonction d'autres critères personnalisés.

6. Sélectionnez une ou plusieurs distributions à associer au trust store. Seules les distributions dont le protocole HTTP3 est désactivé et dont les comportements de HTTPS-only cache sont compatibles avec Viewer MTL.
7. Choisissez Associer.

Associer un trust store via la page des paramètres de distribution :

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution que vous souhaitez associer
3. Sous l'onglet Général, dans le conteneur Paramètres, choisissez Modifier dans le coin supérieur droit
4. Faites défiler la page vers le bas, dans le conteneur de connectivité, activez le commutateur Viewer mTLS
5. Configurez les options mTLS du Viewer disponibles :
   - Mode de validation du certificat client : choisissez entre le mode obligatoire et le mode facultatif. En mode obligatoire, tous les clients sont tenus de présenter des certificats. En mode facultatif, les clients qui présentent des certificats sont validés, tandis que les clients qui ne présentent pas de certificats sont autorisés à y accéder.
   - Publiez les noms des autorités de certification de confiance : choisissez si vous souhaitez annoncer les noms des autorités de certification de votre boutique de confiance aux clients lors de la poignée de main TLS.
   - Ignorer la date d'expiration du certificat : choisissez si vous souhaitez autoriser les connexions avec des certificats expirés (les autres critères de validation s'appliquent toujours).
   - Fonction de connexion : une fonction de connexion optionnelle peut être associée aux allow/deny connexions en fonction d'autres critères personnalisés.
6. Choisissez Enregistrer les modifications dans le coin inférieur droit.

Pour associer un magasin de confiance (AWS CLI)

Les magasins fiduciaires peuvent être associés aux distributions à l'aide de la DistributionConfig.ViewerMtlsConfig propriété. Cela signifie que vous devez d'abord récupérer la configuration de distribution, puis la fournir ViewerMtlsConfig dans une UpdateDistribution demande ultérieure.

```
// First fetch the distribution
aws cloudfront get-distribution {DISTRIBUTION_ID}

// Update the distribution config, for example:
Distribution config, file://distConf.json:
{
  ...other fields,
  ViewerMtlsConfig: {
    Mode: 'required',
    TrustStoreConfig: {
        AdvertiseTrustStoreCaNames: false,
        IgnoreCertificateExpiry: true,
        TrustStoreId: {TRUST_STORE_ID}
    }
  }
}

aws cloudfront update-distribution \
   --id {DISTRIBUTION_ID} \
   --if-match {ETAG} \
   --distribution-config file://distConf.json
```

Gérez les magasins de confiance

Afficher les détails de Trust Store

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Trust stores.
3. Choisissez le nom du trust store pour afficher sa page de détails.

La page de détails présente :

- Nom et identifiant du magasin de confiance
- Nombre de certificats CA
- Date de création et date de dernière modification
- Distributions associées
- Étiquettes

Modifier un trust store

Pour remplacer le bundle de certificats CA :

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Trust stores.
3. Choisissez le nom du trust store.
4. Choisissez Actions, puis Modifier.
5. Pour le bundle d'autorité de certification (CA), entrez l'emplacement Amazon S3 du fichier PEM du bundle CA mis à jour.
6. Choisissez Update Trust Store.

Supprimer un trust store

Conditions préalables : vous devez d'abord dissocier le trust store de toutes les CloudFront distributions.

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Trust stores.
3. Choisissez le nom du trust store.
4. Choisissez Supprimer le trust store.
5. Choisissez Supprimer pour confirmer.

Étapes suivantes

Après avoir créé et associé votre trust store à une CloudFront distribution, vous pouvez activer l'authentification TLS mutuelle sur votre distribution et configurer des paramètres supplémentaires tels que le transfert des en-têtes de certificats vers vos origines. Pour obtenir des instructions détaillées sur l'activation des MTLs sur vos distributions, consultezActiver le protocole TLS mutuel pour les distributions CloudFront.

Activer le protocole TLS mutuel pour les distributions CloudFront

Prérequis et exigences

CloudFront le mode de vérification TLS mutuelle exige que tous les clients présentent des certificats valides lors de la prise de contact TLS et rejette les connexions sans certificats valides. Avant d'activer le protocole TLS mutuel sur une CloudFront distribution, assurez-vous d'avoir :

- Création d'un magasin de confiance avec les certificats de votre autorité de certification
- Associez le trust store à votre CloudFront distribution
- Garantie que tous les comportements du cache de distribution utilisent une politique de protocole de HTTPS-only visualisation
- Vous avez vérifié que votre distribution est utilisée HTTP/2 (paramètre par défaut, Viewer mTLS n'est pas pris en charge sur HTTP/3)

> **Note**
>
> L'authentification TLS mutuelle nécessite des connexions HTTPS entre les utilisateurs et CloudFront. Vous ne pouvez pas activer le protocole MTL sur une distribution dont les comportements de cache prennent en charge les connexions HTTP.

Activer le protocole TLS mutuel (console)

Pour les nouvelles distributions

Les fichiers MTL Viewer ne peuvent pas être configurés lors de la création d'une nouvelle distribution dans la CloudFront console. Créez d'abord la distribution par n'importe quel moyen (console, CLI, API), puis modifiez les paramètres de distribution pour activer Viewer MTL conformément aux instructions de distribution existantes ci-dessous.

Pour les distributions existantes

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans la liste de distribution, sélectionnez la distribution que vous souhaitez modifier.
3. Assurez-vous que la politique du protocole Viewer est définie sur Rediriger le HTTP vers HTTPS ou HTTPS uniquement pour tous les comportements du cache. (Vous pouvez choisir

l'onglet Comportements du cache pour afficher et mettre à jour les comportements du cache conformément aux politiques du protocole HTTP.)

4. Choisissez l'onglet Général.
5. Dans la section Settings (Paramètres), choisissez Edit (Modifier).
6. Dans la section Connectivité, recherchez l'authentification mutuelle (mTLS) du visualiseur.
7. Activez Activer l'authentification mutuelle.
8. Pour le mode de validation du certificat client, sélectionnez Obligatoire (tous les clients doivent présenter des certificats) ou Facultatif (les clients peuvent éventuellement présenter des certificats).
9. Pour Trust store, sélectionnez votre trust store créé précédemment.
10. (Facultatif) Activez Advertise trust store CA names si vous souhaitez envoyer des noms CloudFront d'autorité de certification aux clients lors de la prise de contact TLS.
11. (Facultatif) Activez l'option Ignorer la date d'expiration du certificat si vous souhaitez autoriser les connexions avec des certificats expirés.
12. Cliquez sur Enregistrer les modifications.

Activez le protocole TLS mutuel (AWS CLI)

Pour les nouvelles distributions

L'exemple suivant montre comment créer un fichier de configuration de distribution (distribution-config.json) qui inclut les paramètres mTLS :

```
{
  "CallerReference": "cli-example-1",
  "Origins": {
    "Quantity": 1,
    "Items": [
      {
        "Id": "my-origin",
        "DomainName": "example.com",
        "CustomOriginConfig": {
          "HTTPPort": 80,
          "HTTPSPort": 443,
          "OriginProtocolPolicy": "https-only"
        }
      }
    ]
```

```
  },
  "DefaultCacheBehavior": {
    "TargetOriginId": "my-origin",
    "ViewerProtocolPolicy": "https-only",
    "MinTTL": 0,
    "ForwardedValues": {
      "QueryString": false,
      "Cookies": {
        "Forward": "none"
      }
    }
  },
  "ViewerCertificate": {
    "CloudFrontDefaultCertificate": true
  },
  "ViewerMtlsConfig": {
    "Mode": "required",
    "TrustStoreConfig": {
        "TrustStoreId": {TRUST_STORE_ID},
        "AdvertiseTrustStoreCaNames": true,
        "IgnoreCertificateExpiry": true
    }
  },
  "Enabled": true
}
```

Créez la distribution avec mTLS activé à l'aide de l'exemple de commande suivant :

```
aws cloudfront create-distribution --distribution-config file://distribution-
config.json
```

Pour les distributions existantes

Obtenez la configuration de distribution actuelle à l'aide de l'exemple de commande suivant :

```
aws cloudfront get-distribution-config --id E1A2B3C4D5E6F7 --output json > dist-
config.json
```

Modifiez le fichier pour ajouter les paramètres mTLS. Ajoutez la section d'exemple suivante à votre configuration de distribution :

```
"ViewerMtlsConfig": {
```

```
    "Mode": "required",
    "TrustStoreConfig": {
        "TrustStoreId": {TRUST_STORE_ID},
        "AdvertiseTrustStoreCaNames": true,
        "IgnoreCertificateExpiry": true
    }
}
```

Supprimez le champ ETag du fichier mais enregistrez sa valeur séparément.

Mettez à jour la distribution avec la nouvelle configuration à l'aide de l'exemple de commande suivant :

```
aws cloudfront update-distribution \
    --id E1A2B3C4D5E6F7 \
    --if-match YOUR-ETAG-VALUE \
    --distribution-config file://dist-config.json
```

Politiques du protocole Viewer

Lorsque vous utilisez le protocole TLS mutuel, tous les comportements du cache de distribution doivent être configurés avec une politique de protocole de HTTPS-only visualisation :

- Rediriger le HTTP vers HTTPS : redirige les requêtes HTTP vers le protocole HTTPS avant de procéder à la validation du certificat.
- HTTPS uniquement : accepte uniquement les requêtes HTTPS et effectue la validation des certificats.

> **Note**
>
> La politique du protocole d'affichage HTTP et HTTPS n'est pas prise en charge avec le protocole TLS mutuel, car les connexions HTTP ne peuvent pas effectuer de validation de certificat.

Étapes suivantes

Après avoir activé Viewer TLS sur votre CloudFront distribution, vous pouvez associer des fonctions de connexion pour implémenter une logique de validation de certificat personnalisée. Les fonctions

de connexion vous permettent d'étendre les capacités d'authentification mTLS intégrées grâce à des règles de validation personnalisées, à la vérification de la révocation des certificats et à la journalisation. Pour plus de détails sur la création et l'association de fonctions de connexion, consultezAssocier une fonction CloudFront de connexion.

Associer une fonction CloudFront de connexion

CloudFront Les fonctions de connexion vous permettent de mettre en œuvre une logique de validation de certificat personnalisée lors des connexions TLS, en fournissant des extensions aux fonctionnalités d'authentification MTLS intégrées.

Que sont les fonctions de connexion ?

Les fonctions de connexion sont JavaScript des fonctions qui s'exécutent pendant le handshake TLS une fois que les certificats clients ont été validés. Le certificat client validé est transmis à la fonction de connexion, qui peut alors prendre une décision supplémentaire quant à l'octroi ou non de l'accès. Pour des informations détaillées sur les fonctions de connexion, consultezPersonnalisez avec les fonctions CloudFront de connexion.

Comment les fonctions de connexion fonctionnent avec les MTLs

Lorsqu'un client tente d'établir une connexion mTLS avec votre CloudFront distribution, la séquence suivante se produit :

1. Le client lance une prise de contact TLS avec un CloudFront emplacement périphérique.
2. CloudFront demande et reçoit un certificat client.
3. CloudFront effectue la validation standard des certificats par rapport à Trust Store.
4. Si le certificat passe la validation standard, CloudFront invoque votre fonction de connexion. S'il IgnoreCertificateExpiryest activé dans votre ViewerMtlsConfig, vos certificats expirés (mais valides pour le reste) sont également transmis à la fonction de connexion. Si les certificats clients ne sont pas valides, les fonctions de connexion ne seront pas invoquées.
5. Votre fonction de connexion reçoit les informations de certificat et les détails de connexion analysés.
6. Votre fonction prend une allow/deny décision basée sur une logique personnalisée.
7. CloudFront termine ou met fin à la connexion TLS selon votre décision.

Les fonctions de connexion sont invoquées à la fois pour le mode de vérification et le mode facultatif (lorsque les clients présentent des certificats).

Création d'une fonction de connexion

Vous pouvez créer des fonctions de connexion à l'aide de la CloudFront console ou de la AWS CLI.

Pour créer une fonction de connexion (console)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Fonctions.
3. Choisissez l'onglet Fonctions de connexion, puis sélectionnez Créer une fonction de connexion.
4. Entrez un nom de fonction unique au sein de votre AWS compte.
5. Sélectionnez Continuer.
6. Dans l'éditeur de fonctions, écrivez votre JavaScript code pour la validation du certificat. Le gestionnaire de fonctions doit appeler allow ou deny.
7. Facultatif : un KeyValue magasin peut être associé à la fonction de connexion pour implémenter le contrôle de révocation.
8. Cliquez sur Enregistrer les modifications.

Pour créer une fonction de connexion (AWS CLI)

L'exemple suivant montre comment créer une fonction de connexion :

Écrivez le code de votre fonction dans un fichier séparé, par exemple code.js :

```
function connectionHandler(connection) {
  connection.allow();
}
```

```
aws cloudfront create-connection-function \
  --name "certificate-validator" \
  --connection-function-config '{
      "Comment": "Client certificate validation function",
      "Runtime": "cloudfront-js-2.0"
  }' \
  --connection-function-code fileb://code.js
```

Structure du code de la fonction de connexion

Les fonctions de connexion implémentent la fonction ConnectionHandler qui reçoit un objet de connexion contenant le certificat et les informations de connexion. Votre fonction doit utiliser l'un `connection.allow()` ou `connection.deny()` l'autre ou prendre une décision concernant la connexion.

Exemple de fonction de connexion de base

L'exemple suivant montre une fonction de connexion simple qui vérifie le champ objet des certificats clients :

```
function connectionHandler(connection) {
    // Only process if a certificate was presented
    if (!connection.clientCertificate) {
        console.log("No certificate presented");
        connection.deny();
    }

    // Check the subject field for specific organization
    const subject = connection.clientCertificate.certificates.leaf.subject;
    if (!subject.includes("O=ExampleCorp")) {
        console.log("Certificate not from authorized organization");
       connection.deny();
    } else {
        // All checks passed
        console.log("Certificate validation passed");
        connection.allow();
    }
}
```

La spécification complète des propriétés du certificat client disponibles sur l'objet de connexion est disponible ici :

```
{
  "connectionId": "Fdb-Eb7L9gVn2cFakz7wWyBJIDAD4-oNO6g8r3vXDV132BtnIVtqDA==", // Unique
 identifier for this TLS connection
  "clientIp": "203.0.113.42", // IP address of the connecting client (IPv4 or IPv6)
  "clientCertificate": {
    "certificates": {
      "leaf": {
```

```
      "serialNumber": "4a:3f:5c:92:d1:e8:7b:6c", // Unique serial number assigned by
the issuing CA (hexadecimal)
      "issuer": "CN=Example Corp Intermediate CA,O=Example Corp,C=US", //
Distinguished Name (DN) of the certificate authority that issued this certificate.
      "subject": "CN=client.example.com,O=Example Corp,C=US", // Distinguished Name
(DN) of the certificate holder.
      "validity": {
        "notBefore": "2024-01-15T00:00:00Z", // Certificate validity start date (ISO
8601 format)
        "notAfter": "2025-01-14T23:59:59Z"   // Certificate expiration date (ISO 8601
format)
      },
      "sha256Fingerprint": "a1b2c3d4e5f6...abc123def456", // SHA-256 hash of the
certificate (64 hex characters)
      "ocspEndpoint": "http://ocsp.example.com", // OCSP responder URL from the
certificate's AIA extension.
      "san": "DNS:client.example.com,DNS:api.example.com", // Subject Alternative
Names.
      "spki":
"30820122300d06092a864886f70d01010105000382010f003082010a0282010100...", // Subject
Public Key Info (DER-encoded, hex).
      "sanHex":
"3032820f636c69656e742e6578616d706c652e636f6d820f6170692e6578616d706c652e636f6d..." //
Subject Alternative Names (DER-encoded, hex).
    },
    "intermediates": [
      {
        "serialNumber": "00:d4:04:a5:fd:cb:20:37:54", // Serial number of the
intermediate certificate.
        "issuer": "CN=Example Corp Root CA,O=Example Corp,C=US", // Issuer of the
intermediate certificate.
        "subject": "CN=Example Corp Intermediate CA,O=Example Corp,C=US", // Subject
of the intermediate certificate.
        "validity": {
          "notBefore": "2020-01-01T00:00:00Z",
          "notAfter": "2030-01-01T23:59:59Z"
        },
        "sha256Fingerprint": "b2c3d4e5f6a1...def456abc123",
        "ocspEndpoint": "http://ocsp.example.com/intermediate",
        "san": "DNS:ca.example.com",
        "spki":
"30820122300d06092a864886f70d01010105000382010f003082010a0282010100b389dd513b...",
        "sanHex": "3015820d63612e6578616d706c652e636f6d..."
      }
```

```
      ]
    }
  }
}
```

Associer une fonction de connexion

Après avoir créé votre fonction de connexion, vous devez la publier sur la scène LIVE et l'associer à votre distribution.

Pour publier et associer une fonction de connexion (console)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Functions
3. Choisissez l'onglet Fonctions de connexion et sélectionnez votre fonction de connexion.
4. Choisissez Publier pour le déplacer vers la scène LIVE.
5. Choisissez Ajouter une association dans le tableau des distributions associé situé sous la section de publication.
6. Sélectionnez la distribution à laquelle Viewer mTLS est activé et que vous souhaitez associer.

Les fonctions de connexion publiées de manière alternative peuvent également être associées à partir de la page de détails de distribution.

1. Accédez à la page d'accueil de la console où toutes vos distributions sont répertoriées.
2. Sélectionnez la distribution que vous souhaitez associer.
3. Choisissez l'onglet Général.
4. Dans la section Settings (Paramètres), choisissez Edit (Modifier).
5. Dans la section Connectivité, recherchez l'authentification mutuelle (mTLS) du visualiseur.
6. Pour Fonction de connexion, sélectionnez votre fonction.
7. Cliquez sur Enregistrer les modifications.

Pour associer une fonction de connexion (AWS CLI)

L'exemple suivant montre comment associer une fonction de connexion à une distribution :

```
// DistributionConfig:
{
   ...other settings,
    "ConnectionFunctionAssociation": {
        "Id": "cf_30c2CV2elHwCoInb3LtcaUJkZeD"
    }
}
```

Cas d'utilisation des fonctions de connexion

Les fonctions de connexion permettent plusieurs cas d'utilisation avancés des MTL :

- Validation des attributs de certificat : vérifiez des champs spécifiques dans les certificats clients, tels que les exigences relatives aux unités organisationnelles ou les modèles de noms alternatifs des sujets.
- Vérification de la révocation des certificats - Mettez en œuvre une vérification personnalisée de la révocation des certificats KeyValueStore pour stocker les numéros de série des certificats révoqués.
- IP-based politiques de certification - Appliquez différentes politiques de certification en fonction des adresses IP des clients ou des restrictions géographiques.
- Multi-tenant validation - Mettez en œuvre des règles de validation spécifiques au locataire dans lesquelles différentes exigences en matière de certificat s'appliquent en fonction des noms d'hôte ou des attributs des certificats.

> **Note**
>
> Les fonctions de connexion s'exécutent une fois par connexion client lors de la prise de contact TLS.
> Les fonctions de connexion peuvent uniquement autoriser ou refuser les connexions, pas modifier le protocole HTTP requests/responses.
> Seules les fonctions de scène LIVE (publiées) peuvent être associées aux distributions.
> Chaque distribution peut avoir au plus une fonction de connexion.

Étapes suivantes

Après avoir associé une fonction de connexion à votre CloudFront distribution, vous pouvez configurer des paramètres facultatifs pour personnaliser le comportement de votre implémentation mTLS. Pour obtenir des instructions détaillées sur la configuration de paramètres supplémentaires tels qu'un mode de validation de certificat client facultatif, consultezConfiguration de paramètres supplémentaires.

Configuration de paramètres supplémentaires

Après avoir activé l'authentification TLS mutuelle de base, vous pouvez configurer des paramètres supplémentaires pour personnaliser le comportement d'authentification en fonction de cas d'utilisation et d'exigences spécifiques.

Publicité de l'autorité de certification

Le AdvertiseTrustStoreCaNames champ contrôle si CloudFront la liste des noms d'autorités de certification fiables est envoyée aux clients lors de la prise de contact TLS, afin d'aider les clients à sélectionner le certificat approprié.

Pour configurer la publicité CA (console)

1. Dans vos paramètres de distribution, accédez à l'onglet Général, puis choisissez Modifier.
2. Accédez à la section Authentification mutuelle (mTLS) du visualiseur dans le conteneur de connectivité.
3. Cochez ou désélectionnez la case Advertise Trust Store CA names.
4. Cliquez sur Enregistrer les modifications.

Pour configurer la publicité CA (AWS CLI)

L'exemple suivant montre comment activer la publicité CA :

```
"ViewerMtlsConfig": {
   "Mode": "required", // or "optional"
   "TrustStoreConfig": {
      "AdvertiseTrustStoreCaNames": true,
      ...other settings
   }
```

```
}
```

Gestion de l'expiration des certificats

La IgnoreCertificateExpiry propriété détermine le mode CloudFront de réponse aux certificats clients expirés. Par défaut, CloudFront rejette les certificats clients expirés, mais vous pouvez le configurer pour les accepter si nécessaire. Ceci est généralement activé pour les appareils dont les certificats ont expiré et qui ne peuvent pas être facilement mis à jour.

Pour configurer la gestion de l'expiration des certificats (console)

1. Dans vos paramètres de distribution, accédez à l'onglet Général, puis choisissez Modifier.
2. Accédez à la section Authentification mutuelle (mTLS) Viewer du conteneur de connectivité.
3. Cochez ou désélectionnez la case Ignorer la date d'expiration du certificat.
4. Cliquez sur Enregistrer les modifications.

Pour configurer la gestion de l'expiration des certificats (AWS CLI)

L'exemple suivant montre comment ignorer l'expiration d'un certificat :

```
"ViewerMtlsConfig": {
  "Mode": "required", // or "optional"
  "TrustStoreConfig": {
     "IgnoreCertificateExpiry": false,
     ...other settings
  }
}
```

> **Note**
>
> IgnoreCertificateExpirys'applique uniquement aux dates de validité des certificats. Tous les autres contrôles de validation des certificats s'appliquent toujours (chaîne de confiance, validation de signature).

Étapes suivantes

Après avoir configuré des paramètres supplémentaires, vous pouvez configurer le transfert d'en-têtes pour transmettre les informations de certificat à vos origines, implémenter la révocation des certificats

à l'aide des fonctions de connexion et KeyValueStore activer les journaux de connexion à des fins de surveillance. Pour plus de détails sur le transfert des informations de certificat vers les origines, voir Transférer les en-têtes vers les origines.

En-têtes MTLS Viewer pour les politiques de cache et transférés à l'origine

Lorsque vous utilisez l'authentification TLS mutuelle, CloudFront vous pouvez extraire des informations des certificats clients et les transmettre à vos origines sous forme d'en-têtes HTTP. Cela permet à vos serveurs d'origine d'accéder aux détails des certificats sans implémenter de logique de validation des certificats.

Les en-têtes suivants sont disponibles pour créer des comportements de cache :

Nom de l'en-tête	Description	Exemple de valeur	Modes pris en charge
CloudFront-Viewer-Cert-Serial-Number	Représentation hexadécimale du numéro de série du certificat	4a : 3 f : 5 c : 92 : d : e 8 : 7 b : 6 c	Obligatoire, facultatif, transmission
CloudFront-Viewer-Cert-Issuer	Représentation sous forme de chaîne RFC2253 du nom distinctif (DN) de l'émetteur	CN=Rootca mtls.com, OU = Rootca, O = MTLS, L = Seattle, ST = Washington, C = États-Unis	Obligatoire, facultatif, transmission
CloudFront-Viewer-Cert-Subject	Représentation sous forme de chaîne RFC2253 du nom distinctif (DN) du sujet	CN=Client_.com, OU = Client-3, O = MTLS, ST = Washington, C = États-Unis	Obligatoire, facultatif, transmission
CloudFront-Viewer-Cert-Present	1 (présent) ou 0 (absent) indiquant si le certificat est présent. Cette valeur est toujours égale à 1 en mode obligatoire.	1	Obligatoire, facultatif, transmission

Nom de l’en-tête	Description	Exemple de valeur	Modes pris en charge
CloudFront-Viewer-Cert-Sha256	Le hachage SHA256 du certificat client	01fbf94fe f55697534 20c349f49 adbfd80af 527537781 6e3ab1fb3 71b29cb586	Obligatoire, facultatif, transmission

Pour les demandes d'origine, deux en-têtes supplémentaires sont fournis, en plus des en-têtes ci-dessus mis à disposition pour les comportements du cache. En raison de la taille potentielle de l' CloudFront-Viewer-Cert-Pem en-tête, l'en-tête n'est pas exposé aux fonctions périphériques (Lambda @Edge ou CloudFront Functions) et est uniquement transmis à l'origine.

Nom de l’en-tête	Description	Exemple de valeur	Modes pris en charge
CloudFront-Viewer-Cert-Validity	Format ISO8601 des dates NotBefore et NotAfter	CloudFront-Viewer-Cert-Validity: NotBefore =21/09/2023 ; =20/09/2024 T01:50:17Z NotAfter T01:50:17 Z	Obligatoire, facultatif, transmission
CloudFront-Viewer-Cert-Pem	URL-encoded Format PEM du certificat feuille	CloudFront-Viewer-Cert-Pem: ----- BEGIN%20CERTIFICATE----- %0AMIIG<... réduit... > NmrUlw %0A----END	Obligatoire, facultatif

Nom de l’en-tête	Description	Exemple de valeur	Modes pris en charge
		%20CERTI FICAT----------A	
Client-Cert	Certificat Leaf	Client-Ce rt: :MIIG<... réduit... > NmrUlw :	Transmettre
Client-Cert-Chain	Non-leaf chaîne de certificats	Client-Cert-Chain: :MIIG<... réduit... > NmrUlw :	Transmettre

Configurer le transfert d'en-têtes

Console

En mode vérification, ajoute CloudFront automatiquement les en-têtes CloudFront-Viewer-Cert -* à toutes les demandes des utilisateurs. Pour transférer ces en-têtes vers votre source :

1. Sur la page principale des distributions de la liste, sélectionnez votre distribution avec les lecteurs MTL activés et accédez à l'onglet Comportements
2. Sélectionnez le comportement du cache et choisissez Modifier
3. Dans la section Politique de demande d'origine, choisissez Créer une politique ou sélectionnez une politique existante
4. Assurez-vous que les en-têtes suivants sont inclus dans la politique de demande d'origine :
   - CloudFront-Viewer-Cert-Serial-Number
   - CloudFront-Viewer-Cert-Issuer
   - CloudFront-Viewer-Cert-Subject
   - CloudFront-Viewer-Cert-Present
   - Cloudfront-Viewer-Cert-Sha256
   - CloudFront-Viewer-Cert-Validity
   - CloudFront-Viewer-Cert-Pem

5. Choisissez Créer (pour les nouvelles politiques) ou Enregistrer les modifications (pour les politiques existantes)
6. Sélectionnez la politique dans le comportement de votre cache et enregistrez les modifications

Utilisation AWS INTERFACE DE LIGNE DE COMMANDE (CLI)

L'exemple suivant montre comment créer une politique de demande d'origine qui inclut les en-têtes mTLS pour le mode vérification :

```
aws cloudfront create-origin-request-policy \
  --origin-request-policy-config '{
    "Name": "MTLSHeadersPolicy",
    "HeadersConfig": {
      "HeaderBehavior": "whitelist",
      "Headers": {
        "Quantity": 5,
        "Items": [
          "CloudFront-Viewer-Cert-Serial-Number",
          "CloudFront-Viewer-Cert-Issuer",
          "CloudFront-Viewer-Cert-Subject",
          "CloudFront-Viewer-Cert-Validity",
          "CloudFront-Viewer-Cert-Pem"
        ]
      }
    },
    "CookiesConfig": {
      "CookieBehavior": "none"
    },
    "QueryStringsConfig": {
      "QueryStringBehavior": "none"
    }
  }'
```

Considérations relatives au traitement des en-

Lorsque vous travaillez avec des en-têtes de certificat, tenez compte des meilleures pratiques suivantes :

- Validation des en-têtes : vérifiez les valeurs des en-têtes des certificats à l'origine comme mesure de sécurité supplémentaire

- Limites de taille des en-têtes : les en-têtes des certificats PEM peuvent être volumineux, assurez-vous que votre serveur d'origine peut les gérer
- Considérations relatives au cache : l'utilisation d'en-têtes de certificat dans votre clé de cache augmente la fragmentation du cache
- Cross-origin demandes : si votre application utilise le CORS, vous devrez peut-être le configurer pour autoriser les en-têtes de certificat

Étapes suivantes

Après avoir configuré le transfert d'en-têtes, vous pouvez implémenter la vérification de révocation des certificats à l'aide des fonctions de CloudFront connexion et KeyValueStore. Pour plus de détails sur la mise en œuvre des contrôles de révocation, consultezRévocation du certificat.

Révocation du certificat

Lorsque des certificats doivent être révoqués, en raison de compromissions, de modifications de politique ou de résiliation de relations, vous avez besoin d'un mécanisme permettant de rejeter ces certificats lors de la poignée de main des MTL. CloudFront propose deux approches natives pour la révocation des certificats, que vous pouvez combiner pour un contrôle en couches.

- OCSP (Online Certificate Status Protocol) : CloudFront interroge le répondeur OCSP de votre autorité de certification en temps réel pour vérifier si un certificat client a été révoqué. Activez OCSP sur votre magasin de confiance et gérez la CloudFront validation automatiquement lors de la prise de contact TLS. Les résultats OCSP sont également visibles dans Connection Functions, ce qui vous donne un accès programmatique au statut de révocation pour une prise de décision personnalisée.
- CloudFront Fonctions et KeyValueStore — Vous maintenez une liste des numéros de série des certificats révoqués dans un CloudFront KeyValueStore. Une fonction de connexion interroge le KeyValueStore pendant la prise de contact TLS et autorise ou refuse la connexion. Cela vous donne un contrôle total sur les données de révocation, le calendrier des mises à jour et la logique personnalisée telle que les délais de grâce ou les IP-based exceptions.

Comparaison : OCSP et CloudFront fonctions avec KeyValueStore

	OCSP	CloudFront Fonctions + KeyValueStore
Source de données	Répondeur OCSP de l'autorité de certification	Vous gérez la liste de révocation
Mécanisme de mise à jour	Real-time requête à CA	Vous envoyez les mises à jour à KeyValueStore
Logique personnalisée	Disponible à l'aide des fonctions de connexion	Intégré à votre code de fonction
Dépendance externe	Nécessite la disponibilité du répondeur CA OCSP	Aucune dépendance externe
Idéal pour	CA qui assurent la maintenance des répondeurs OCSP ; état en temps réel CA-authoritative	Self-managed révocation ; politiques personnalisées ; autorités de certification sans support OCSP

Vous pouvez utiliser les deux approches ensemble. Activez OCSP pour le contrôle de CA-authoritative révocation, puis utilisez une fonction de connexion pour ajouter une logique supplémentaire au résultat OCSP, par exemple en autorisant les certificats révoqués provenant de plages d'adresses IP fiables pendant une période de grâce.

OCSP (protocole d'état des certificats en ligne)

L'OCSP est un protocole en temps réel qui vérifie le statut de révocation d'un certificat directement auprès de l'autorité de certification (CA). Au cours du processus de signature du certificat, l'autorité de certification intègre une URL de répondeur OCSP dans le certificat. Lorsqu'un client présente son certificat lors de la prise de contact mTLS, CloudFront envoie une demande OCSP à l'URL du répondeur intégré et agit en fonction de la réponse : les certificats valides continuent, les certificats révoqués sont résiliés.

CloudFront valide l'ensemble de la chaîne de certificats (le certificat principal et jusqu'à trois certificats intermédiaires) par rapport à leurs URL de répondeur OCSP respectives. Les certificats du trust store sont traités comme des ancres de confiance et sont exclus de la validation OCSP. Cela s'applique à tous les certificats du trust store, qu'il s'agisse d'une autorité de certification racine ou

intermédiaire. Lorsque vous placez une autorité de certification intermédiaire dans votre magasin de confiance, elle devient un point d'ancrage de confiance et la validation en chaîne prend fin avec ce certificat. Seuls les certificats situés en dessous de la chaîne le sont OCSP-validated.

Activer OCSP

Activez OCSP sur votre magasin de confiance. Lorsque cette option est activée, effectue CloudFront automatiquement la validation OCSP pour tout certificat client contenant une URL de répondeur OCSP dans son extension Authority Information Access (AIA). Une fois l'OCSP activé, chaque certificat de la chaîne de certificats client située sous l'ancre de confiance doit avoir une URL OCSP. Si un certificat situé sous l'ancre de confiance ne contient pas d'URL OCSP, la connexion CloudFront n'est pas établie. Les certificats du trust store (Trust Anchors) sont exemptés de cette obligation.

CloudFront met en cache les réponses OCSP à la périphérie afin de réduire le temps d'aller-retour et de se protéger contre les temps d'arrêt du répondeur OCSP. Les réponses OCSP sont mises en cache pendant environ 30 minutes, et le statut de révocation mis à jour peut prendre jusqu'à 30 minutes pour être reflété.

L'OCSP génère des fonctions de connexion

Lorsqu'une fonction de connexion est configurée sur la même distribution, elle l' CloudFrontinvoque une fois la validation OCSP terminée. L'objet de connexion contient le statut OCSP pour les certificats Leaf et intermédiaire :

```
{
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "subject": "CN=client.example.com, O=Example Org",
        "issuer": "CN=Intermediate CA, O=Example Org",
        "serialNumber": "00:a7:30:9e:73:7b:3e:63:bd:b7:c0:7e:bf:d5:c9:86",
        "validity": {
          "notBefore": "2024-01-01T00:00:00Z",
          "notAfter": "2025-01-01T00:00:00Z"
        },
        "sha256Fingerprint":
 "AB:CD:EF:12:34:56:78:90:AB:CD:EF:12:34:56:78:90:AB:CD:EF:12:34:56:78:90:AB:CD:EF:12:34:56:78:
        "ocspEndpoint": "http://ocsp.example.org"
      },
      "intermediates": [
        {
```

```
          "subject": "CN=Intermediate CA, O=Example Org",
          "issuer": "CN=Root CA, O=Example Org",
          "serialNumber": "00:a7:30:9e:73:7b:3e:63:bd:b7:c0:7e:bf:d5:c9:86",
          "validity": {
            "notBefore": "2020-01-01T00:00:00Z",
            "notAfter": "2030-01-01T00:00:00Z"
          },
          "sha256Fingerprint":
 "12:34:56:78:90:AB:CD:EF:12:34:56:78:90:AB:CD:EF:12:34:56:78:90:AB:CD:EF:12:34:56:78:90:AB:CD:
          "ocspEndpoint": "http://ocsp.example.org"
        }
      ]
    },
    "revocationStatus": {
      "chainValidity": "Valid",           // "Valid" | "Invalid" | "Unknown"
      "certificates": {
        "leaf": {
          "method": "OCSP",               // "OCSP"
          "status": "Good",               // "Good" | "Revoked" | "Unknown" | "Error"
          "serialNumber": "00:a7:30:9e:73:7b:3e:63:bd:b7:c0:7e:bf:d5:c9:86"
        },
        "intermediates": [
          {
            "method": "OCSP",             // "OCSP"
            "status": "Error",            // "Good" | "Revoked" | "Unknown" | "Error"
            "errorType": "InternalError", // "InternalError" | "OCSP response
 verification failed: {Type}"
            "serialNumber": "00:a7:30:9e:73:7b:3e:63:bd:b7:c0:7e:bf:d5:c9:86"
          }
        ]
      }
    }
  },
  "clientIp":"127.0.0.1",
  "endpoint":"d123.cloudfront.net",
  "distributionId":"E1NXS4MQZH501R",
  "connectionId":"xdzQ6lJUDUt8b7OuqOD8lmzOC9HcMaXPmhH5ZdzLCZpKxqzfCPpR4A=="
}
```

Le `chainValidity` champ peut être `Valid``Invalid`, ou`Unknown`. Les `status` valeurs de certificat individuelles peuvent être `Good``Revoked`,`Unknown`, ou`Error`. Le `errorType` champ contient `InternalError` ou `OCSP response verification failed: {Type}` lorsque le statut est`Error`.

La fonction de connexion peut annuler le résultat OCSP, par exemple en autorisant un certificat révoqué appartenant à une plage d'adresses IP fiables ou en refusant un certificat que l'OCSP considère comme « bon » sur la base d'une logique métier supplémentaire.

> **Note**
>
> Le `errorType` champ ne sera présent que si le statut l'est`Error`.

Exemple : gestion OCSP personnalisée avec exception IP sécurisée

```
function connectionHandler(connection) {
    var revocationStatus = connection.clientCertificate.revocationStatus;
    var trustedIP = (connection.clientIp === "[IP_ADDRESS]");

    if (revocationStatus.chainValidity === "Invalid") {
        if (trustedIP) {
            connection.allow();
        } else {
            connection.deny();
        }
    } else if (revocationStatus.certificates.leaf.status === "Error") {
        console.log(revocationStatus.certificates.leaf.errorType);
        connection.deny();
    } else {
        connection.allow();
    }
}
```

Comportement de défaillance de l'OCSP

Lorsqu'il est CloudFront impossible de déterminer le statut de révocation d'un certificat (parce que le répondeur OCSP est inaccessible, renvoie une erreur ou renvoie « inconnu »), la connexion est refusée par CloudFront défaut. Pour implémenter un comportement d'échec progressif, utilisez une fonction de connexion. Les fonctions de connexion ne seront pas exécutées si l'OCSP est activé et si l'URL OCSP est absente des certificats clients. Le résultat OCSP est disponible dans l'objet de connexion, et votre fonction peut autoriser les connexions lorsque le statut OCSP est indéterminé :

```
async function connectionHandler(connection) {
    var revocationStatus = connection.clientCertificate.revocationStatus;
```

```
    if (revocationStatus.certificates.leaf.status === "Error" ||
        revocationStatus.certificates.leaf.status === "Unknown") {
        // OCSP responder unreachable — allow connection (soft-fail)
        connection.logCustomData(`OCSP_SOFT_FAIL:
${revocationStatus.certificates.leaf.errorType}`);
        return connection.allow();
    }

    if (revocationStatus.chainValidity === "Invalid") {
        return connection.deny();
    }

    return connection.allow();
}
```

Révocation du certificat avec CloudFront Functions et KeyValueStore

Vous pouvez utiliser les fonctions de CloudFront connexion KeyValueStore pour implémenter la vérification de révocation des certificats sans aucune dépendance externe. Vous conservez une liste des numéros de série des certificats révoqués dans un KeyValueStore, et votre fonction de connexion compare chaque certificat client à cette liste lors de la prise de contact TLS.

Le processus de révocation des certificats se déroule comme suit :

1. Stockez les numéros de série des certificats révoqués dans un CloudFront KeyValueStore.
2. Lorsqu'un client présente un certificat, votre fonction de connexion est invoquée.
3. La fonction compare le numéro de série du certificat au KeyValueStore.
4. Si le numéro de série se trouve dans le magasin, le certificat est révoqué.
5. Votre fonction refuse la connexion pour les certificats révoqués.

Cette approche permet de vérifier les révocations en temps quasi réel sur le réseau périphérique CloudFront mondial.

Pour mettre en œuvre cette approche, vous devez :

- Une distribution configurée avec les lecteurs MTL de visualisation
- A KeyValueStore contenant les numéros de série des certificats révoqués
- Une fonction de connexion qui interroge le KeyValueStore pour vérifier l'état du certificat

Lorsqu'un client se connecte, CloudFront valide le certificat par rapport au trust store, puis exécute votre fonction de connexion. Votre fonction vérifie le numéro de série du certificat par rapport au KeyValueStore et autorise ou refuse la connexion.

Étape 1 : Création d'un formulaire KeyValueStore pour les certificats révoqués

Préparez les numéros de série de vos certificats révoqués au format JSON :

```
{
  "data": [
    { "key": "ABC123DEF456", "value": "" },
    { "key": "789XYZ012GHI", "value": "" }
  ]
}
```

Téléchargez ce fichier JSON dans un compartiment S3, puis créez KeyValueStore :

```
aws s3 cp revoked-serials.json s3://your-bucket-name/revoked-serials.json

aws cloudfront create-key-value-store \
  --name revoked-serials-kvs \
  --import-source '{
    "SourceType": "S3",
    "SourceARN": "arn:aws:s3:::your-bucket-name/revoked-serials.json"
  }'
```

Attendez que le KeyValueStore provisionnement soit terminé. Vérifiez le statut avec :

```
aws cloudfront get-key-value-store --name "revoked-serials-kvs"
```

Étape 2 : Création de la fonction de connexion de révocation

Créez une fonction de connexion qui vérifie les numéros de série des certificats par rapport aux KeyValueStore :

```
aws cloudfront create-connection-function \
  --name "revocation-control" \
  --connection-function-config file://connection-function-config.json \
  --connection-function-code file://connection-function-code.txt
```

Le fichier de configuration indique l' KeyValueStore association :

```
{
  "Runtime": "cloudfront-js-2.0",
  "Comment": "A function that implements revocation control via KVS",
  "KeyValueStoreAssociations": {
    "Quantity": 1,
    "Items": [
      {
        "KeyValueStoreArn": "arn:aws:cloudfront::account-id:key-value-store/kvs-id"
      }
    ]
  }
}
```

Exemple de code de fonction de connexion :

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Get client serial number from client certificate
    const clientSerialNumber =
        connection.clientCertificate.certificates.leaf.serialNumber;

    // Check KVS to see if serial number exists as a key
    // Remove : from the clientSerialNumber if KVS entries dont have it
    const serialNumberExistsInKvs =
        await kvsHandle.exists(clientSerialNumber.replaceAll(":", ""));

    // Deny connection if serial number exists in KVS
    if (serialNumberExistsInKvs) {
        console.log("Connection denied – certificate revoked");
        connection.logCustomData("Connection denied – certificate revoked");
        return connection.deny();
    }

    // Allow connections that don't exist in KVS
    console.log("Connection allowed");
    return connection.allow();
}
```

Étape 3 : Testez votre fonction de révocation

Utilisez la CloudFront console pour tester votre fonction de connexion à l'aide d'exemples de certificats. Accédez à la fonction de connexion dans la console et utilisez l'onglet Test.

- Collez un exemple de certificat au format PEM dans l'interface de test.
- Spécifiez éventuellement une adresse IP client pour tester IP-based la logique.
- Choisissez la fonction Test pour voir les résultats de l'exécution.
- Consultez les journaux d'exécution pour vérifier la logique de votre fonction.

Testez avec des certificats valides et révoqués pour vous assurer que votre fonction gère correctement les deux scénarios.

Étape 4 : associer la fonction à votre distribution

Après avoir publié votre fonction de connexion, associez-la à votre TLS-enabled distribution m pour activer le contrôle de révocation des certificats. Accédez à vos paramètres de distribution, accédez à la section « Authentification mutuelle des spectateurs (mTLS) », sélectionnez votre fonction de connexion et enregistrez les modifications.

Stratégies de révocation avancées

Combinez l'OCSP avec la logique de la fonction de connexion

Vous pouvez activer OCSP pour la vérification des CA-authoritative révocations et ajouter une fonction de connexion par-dessus pour des politiques personnalisées. La fonction de connexion reçoit le résultat OCSP et peut appliquer une logique supplémentaire :

- Périodes de grâce : autorisez les certificats révoqués sur les réseaux internes pendant une période définie lors de la rotation des certificats.
- Accès d'urgence : autorisez les connexions à partir d'adresses IP spécifiques même lorsque l'OCSP signale un statut révoqué.
- Logique de refus personnalisée : bloquez les certificats que l'OCSP considère comme « bons » sur la base de vos propres données de révocation. KeyValueStore

Example Révocation combinée OCSP + KVS

```
import cf from 'cloudfront';
```

```
async function connectionHandler(connection) {
    var kvsHandle = cf.kvs();
    var revocationStatus = connection.clientCertificate.revocationStatus;
    var serialNumber = connection.clientCertificate.certificates.leaf.serialNumber;

    // Check your own revocation list first (immediate revocation, no cache delay)
    var inKvs = await kvsHandle.exists(serialNumber.replaceAll(":", ""));
    if (inKvs) {
        connection.logCustomData("KVS_REVOKED:" + serialNumber);
        return connection.deny();
    }

    // Then check OCSP result
    if (revocationStatus.chainValidity === 'Valid' &&
 revocationStatus.certificates.leaf.status === "Revoked") {
        // OCSP says revoked — allow grace period from trusted IPs
        if (connection.clientIp.startsWith("10.0.")) {
            connection.logCustomData("GRACE_PERIOD:" + serialNumber + ":" +
 connection.clientIp);
            return connection.allow();
        }
        connection.logCustomData("OCSP_REVOKED:" + serialNumber);
        return connection.deny();
    }

    connection.allow();
}
```

Ce modèle permet une révocation immédiate en utilisant KVS (aucun délai de cache) et une CA-authoritative révocation en utilisant OCSP, avec une gestion personnalisée des exceptions entre les deux.

Méthodes auxiliaires pour le protocole TLS mutuel

Utilisez les fonctions d'`cf.mtls`assistance des fonctions de demande du visualiseur pour renommer, reformater ou combiner les en-têtes des certificats clients avant de transférer la demande à votre source. Pour plus de détails, consultez the section called “Méthodes auxiliaires pour le protocole TLS mutuel”.

Modes de validation supplémentaires

Le mode requis est le mode par défaut pour le protocole TLS CloudFront mutuel : il CloudFront valide chaque certificat client et refuse les connexions qui échouent. Toutefois, pour prendre en charge des cas d'utilisation supplémentaires, tels que des applications desservant à la fois des clients m TLS-authenticated et des clients non authentifiés, ou des environnements dans lesquels le serveur d'origine effectue sa propre validation mTLS, la prise en charge de deux modes supplémentaires est prise CloudFront en charge.

Le mode optionnel est conçu pour les applications avec des populations de clients mixtes. Par exemple, un portail qui diffuse du contenu public à des navigateurs non authentifiés tout en limitant les points de terminaison de l'API aux clients présentant des certificats valides. Ou un scénario de migration dans lequel vous intégrez progressivement les clients à mTLS et devez autoriser les connexions authentifiées et non authentifiées pendant la transition.

Le mode Passthrough est conçu pour les clients dont les serveurs d'origine effectuent déjà la validation mTLS. Par exemple, les services qui migrent depuis des proxys inverses locaux, d'autres CDN ou des équilibreurs de charge d'application qui gèrent déjà la vérification des certificats. Le mode Passthrough permet à ces clients de se placer CloudFront en tête de leurs applications sans avoir à réimplémenter la logique de validation à la périphérie.

Mode optionnel

Validation du certificat client Mode optionnel

CloudFront propose un autre mode facultatif de validation des certificats clients qui valide les certificats clients présentés mais autorise l'accès aux clients qui n'en présentent pas.

Comportement en mode facultatif

- Autorise la connexion aux clients possédant des certificats valides (les certificats non valides sont refusés).
- Permet la connexion à des clients sans certificat.
- Permet des scénarios d'authentification client mixtes via une distribution unique.

Le mode optionnel est idéal pour la migration progressive vers l'authentification mTLS, la prise en charge des clients avec des certificats et des clients sans certificat, ou le maintien de la rétrocompatibilité avec les clients existants.

> **Note**
>
> En mode facultatif, les fonctions de connexion sont toujours invoquées même lorsque les clients ne présentent pas de certificats. Vous pouvez ainsi implémenter une logique personnalisée, telle que la journalisation des adresses IP des clients ou l'application de politiques différentes en fonction de la présentation des certificats.

Pour configurer le mode optionnel (console)

1. Dans vos paramètres de distribution, accédez à l'onglet Général, puis choisissez Modifier.
2. Accédez à la section Viewer Mutual Authentication (mTLS) dans le conteneur Connectivity.
3. Pour le mode de validation du certificat client, sélectionnez Facultatif.
4. Enregistrez les modifications.

Pour configurer le mode optionnel (AWS CLI)

L'exemple suivant montre comment configurer le mode optionnel :

```
"ViewerMtlsConfig": {
    "Mode": "optional",
    ...other settings
}
```

Personnaliser les en-têtes de certificat

Utilisez les fonctions d'assistance mTLS dans Viewer-request CloudFront Functions pour renommer, reformater ou combiner les en-têtes de certificat avant qu'ils n'atteignent votre origine. Cela est utile lors de la migration depuis d'autres services utilisant des noms d'en-tête ou des formats de codage de certificats différents.

Mode Passthrough

Avec le mode passthrough, vous pouvez utiliser CloudFront vos implémentations mTLS existantes à votre origine. CloudFront met fin à la connexion TLS et transmet le certificat client à votre origine sous forme d'en-têtes HTTP. Votre origine effectue toutes les validations des certificats, y compris la vérification de la chaîne, la vérification de la révocation et l'application de politiques personnalisées.

Comment fonctionne le mode passthrough

1. Le client se connecte à un certificat client CloudFront et le présente lors de la prise de contact TLS.
2. CloudFront termine la prise de contact TLS sans valider le certificat auprès d'un magasin de confiance.
3. CloudFront ajoute le certificat client et la chaîne de certificats en tant qu'en-têtes HTTP à la demande.
4. La demande est transmise à votre point d'origine. Aucun contenu n'est mis en cache.
5. Votre origine valide le certificat et traite la demande.

Les clients peuvent également se connecter sans présenter de certificat. Votre fonction d'origine ou de connexion gère les scénarios de certificats vides.

> **Note**
>
> En mode relais, les fonctions de connexion sont toujours invoquées même lorsque les clients ne présentent pas de certificats. Vous pouvez ainsi implémenter une logique personnalisée, telle que la journalisation des adresses IP des clients ou l'application de politiques différentes en fonction de la présentation des certificats.

Exigences de configuration

- Pas de magasin de confiance — La distribution doit avoir des associations de magasins zéro confiance.
- Mise en cache désactivée : tous les comportements de cache doivent utiliser la politique de `CachingDisabled` cache gérée.
- Origin Shield interdit — Origin Shield ne peut pas être activé.
- Lambda @Edge interdit — Les associations de fonctions Lambda @Edge ne sont pas autorisées.
- Politique de demande d'origine requise : vous devez autoriser les `Client-Cert-Chain` en-têtes `Client-Cert` et dans votre politique de demande d'origine pour que l'origine les reçoive.
- Certificate-chain-depth— CloudFront permet une profondeur maximale de 4 pour la transmission de la chaîne de certificats clients aux origines.

Activer le mode passthrough

Console

1. Mettez à jour tous les comportements du cache pour utiliser la politique de `CachingDisabled` cache gérée.
2. Ouvrez la CloudFront console et choisissez votre distribution.
3. Choisissez l'onglet Général, puis choisissez Modifier sous Paramètres.
4. Sous Authentification mutuelle du visualiseur (mTLS), sélectionnez Passthrough.
5. Cliquez sur Enregistrer les modifications.

AWS INTERFACE DE LIGNE DE COMMANDE (CLI)

Assurez-vous que tous les comportements du cache font référence à la `CachingDisabled` politique gérée, puis mettez à jour la configuration de distribution :

```
{
  "ViewerMtlsConfig": {
    "Mode": "passthrough"
  }
}
```

En-têtes transférés à l'origine

CloudFront ajoute les en-têtes suivants à la demande envoyée à votre origine :

- `Client-Cert`— Le certificat d'entité finale (feuille) présenté par le client, codé en base64.
- `Client-Cert-Chain`— La chaîne de certificats (à l'exclusion de la feuille), sous forme de liste de champs structurée. Chaque certificat est codé en base64. `Client-Cert-Chain`est un en-tête de type Liste. Il peut apparaître plusieurs fois dans une demande. La concaténation de toutes les valeurs préserve l'ordre de chaîne d'origine. `Client-Cert-Chain`est omis lorsque le client ne présente qu'un seul certificat.

CloudFront supprime tous les `Client-Cert-Chain` en-têtes entrants `Client-Cert` ou provenant de la demande du client avant d'ajouter les données de certificat réelles. Cela permet d'éviter l'usurpation d'en-tête.

Personnaliser les en-têtes de certificat

Utilisez les fonctions d'assistance mTLS dans Viewer-request CloudFront Functions pour renommer, reformater ou combiner les en-têtes de certificat avant qu'ils n'atteignent votre origine. Cela est utile lors de la migration depuis d'autres services utilisant des noms d'en-tête ou des formats de codage de certificats différents.

Observabilité à l'aide des journaux de connexion

CloudFront les journaux de connexion fournissent une visibilité détaillée sur les événements d'authentification TLS mutuels, ce qui vous permet de surveiller la validation des certificats, de suivre les tentatives de connexion et de résoudre les problèmes d'authentification.

Que sont les journaux de connexion ?

Les journaux de connexion capturent des informations détaillées sur les handshakes TLS et la validation des certificats pour les distributions mutuelles. TLS-enabled Contrairement aux journaux d'accès standard qui enregistrent les informations relatives aux requêtes HTTP, les journaux de connexion se concentrent spécifiquement sur la phase d'établissement de la connexion TLS, notamment :

- État de la connexion (success/failure)
- Détails du certificat client
- Protocole TLS et informations de chiffrement
- Métriques de synchronisation des connexions
- Données personnalisées provenant de Connection Functions

Ces journaux fournissent une visibilité complète des événements d'authentification basés sur des certificats, ce qui vous aide à surveiller la sécurité, à résoudre les problèmes et à respecter les exigences de conformité.

Activer les journaux de connexion

Les journaux de connexion ne sont disponibles que pour les distributions où l'authentification TLS mutuelle est activée. Vous pouvez envoyer des journaux de connexion vers plusieurs destinations, notamment CloudWatch Logs, Amazon Data Firehose et Amazon S3.

Conditions préalables

Avant d'activer les journaux de connexion :

- Configurez le protocole TLS mutuel pour votre distribution CloudFront
- Activez les journaux de connexion pour votre CloudFront distribution
- Assurez-vous de disposer des autorisations requises pour la destination de journalisation que vous avez choisie
- Pour la livraison entre comptes, configurez les politiques IAM appropriées

Pour activer les journaux de connexion (console)

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans la liste de distribution, sélectionnez votre TLS-enabled distribution m.
3. Sélectionnez l'onglet Logging (Journalisation).
4. Choisissez Ajouter.
5. Sélectionnez le service pour recevoir vos journaux :
   - CloudWatch Journaux
   - Firehose
   - Amazon S3
6. Pour Destination, sélectionnez la ressource correspondant au service que vous avez choisi :
   - Pour CloudWatch Logs, entrez le nom du groupe de logs
   - Pour Firehose, sélectionnez le flux de diffusion Firehose
   - Pour Amazon S3, entrez le nom du compartiment (éventuellement avec un préfixe)
7. (Facultatif) Configurez des paramètres supplémentaires :
   - Sélection des champs : sélectionnez les champs de journal spécifiques à inclure.
   - Format de sortie : Choisissez entre JSON, Plain, W3C, Raw ou Parquet (S3 uniquement).
   - Délimiteur de champs : spécifiez comment séparer les champs du journal.
8. Choisissez Enregistrer les modifications

Pour activer les journaux de connexion (AWS CLI)

L'exemple suivant montre comment activer les journaux de connexion à l'aide de l' CloudWatch API :

```
# Step 1: Create a delivery source
```

```
aws logs put-delivery-source \
  --name "cf-mtls-connection-logs" \
  --resource-arn "arn:aws:cloudfront::123456789012:distribution/E1A2B3C4D5E6F7" \
  --log-type CONNECTION_LOGS

# Step 2: Create a delivery destination
aws logs put-delivery-destination \
  --name "s3-destination" \
  --delivery-destination-configuration \
  "destinationResourceArn=arn:aws:s3:::amzn-s3-demo-bucket1"

# Step 3: Create the delivery
aws logs create-delivery \
  --delivery-source-name "cf-mtls-connection-logs" \
  --delivery-destination-arn "arn:aws:logs:us-east-1:123456789012:delivery-
destination:s3-destination"
```

> **Note**
>
> Lorsque vous utilisez l' CloudWatch API, vous devez spécifier la région de l'est des États-Unis (Virginie du Nord) (us-east-1) même lorsque vous livrez des journaux à d'autres régions.

Champs du journal de connexion

Les journaux de connexion contiennent des informations détaillées sur chaque tentative de connexion TLS :

Champ	Description	Exemple
`eventTimestamp`	Horodatage ISO 8601 lorsque la connexion a été établie ou a échoué	1731620046814
`connectionId`	Identifiant unique pour la connexion TLS	`oLHiEKbQSn8lkvJfA3D4gFowK3_iZ0g4i5nMUjE1Akod8TuAzn5nzg==`
`connectionStatus`	État de la tentative de connexion mTLS.	`Success` ou `Failed`

Champ	Description	Exemple
`clientIp`	Adresse IP du client qui se connecte	`2001:0db8:85a3:0000:0000:8a2e:0370:7334`
`clientPort`	Port utilisé par le client	12137
`serverIp`	Adresse IP du serveur CloudFront Edge	`99.84.71.136`
`distributionId`	CloudFront ID de distribution	`E2DX1SLDPK0123`
`distributionTenantId`	CloudFront ID du locataire de distribution (le cas échéant)	`dt_2te1Ura9X3R2iCGNjW123`
`tlsProtocol`	Version du protocole TLS utilisée	`TLSv1.3`
`tlsCipher`	Suite de chiffrement TLS utilisée pour la connexion	`TLS_AES_128_GCM_SHA256`
`tlsHandshakeDuration`	Durée de la poignée de main TLS en millisecondes	153
`tlsSni`	Valeur d'indication du nom du serveur issue de la poignée de contact TLS	`d111111abcdef8.cloudfront.net`
`clientLeafCertSerialNumber`	Numéro de série du certificat du client	`00:b1:43:ed:93:d2:d8:f3:9d`
`clientLeafCertSubject`	Champ d'objet du certificat du client	`C=US, ST=WA, L=Seattle, O=Amazon.com, OU=CloudFront, CN=client.test.mtls.net`

Champ	Description	Exemple
`clientLeafCertIssuer`	Champ émetteur du certificat du client	`C=US, ST=WA, L=Seattle, O=Amazon.com, OU=CloudFront, CN=test.mtls.net`
`clientLeafCertValidity`	Période de validité du certificat du client	`NotBefore=2025-06-05T23:28:21Z;NotAfter=2125-05-12T23:28:21Z`
`connectionLogCustomData`	Données personnalisées ajoutées à l'aide des fonctions de connexion	`REVOKED:00:b1:43:ed:93:d2:d8:f3:9d`

Codes d'erreur de connexion

```
Failed:ClientCertMaxChainDepthExceeded
Failed:ClientCertMaxSizeExceeded
Failed:ClientCertUntrusted
Failed:ClientCertNotYetValid
Failed:ClientCertExpired
Failed:ClientCertTypeUnsupported
Failed:ClientCertInvalid
Failed:ClientCertIntentInvalid
Failed:ClientCertRejected
Failed:ClientCertMissing
Failed:ClientCertOcspProcessingError
Failed:ClientCertOcspDenied
Failed:TcpError
Failed:TcpTimeout
Failed:ConnectionFunctionError
Failed:ConnectionFunctionDenied
Failed:Internal
Failed:UnmappedConnectionError
```

Lorsque les connexions échouent, CloudFront enregistre des codes de motif spécifiques :

Code	Description
ClientCertMaxChain DepthExceeded	Profondeur maximale de la chaîne de certificats dépassée
ClientCertMaxSizeExceeded	Taille maximale du certificat dépassée
ClientCertUntrusted	Le certificat n'est pas fiable
ClientCertNotYetValid	Le certificat n'est pas encore valide
ClientCertExpired	Le certificat est expiré
ClientCertTypeUnsupported	Le type de certificat n'est pas pris en charge
ClientCertInvalid	Le certificat n'est pas valide
ClientCertIntentInvalid	L'intention du certificat n'est pas valide
ClientCertRejected	Certificat rejeté par validation personnalisée
ClientCertMissing	Le certificat est manquant
TcpError	Une erreur s'est produite lors de la tentative d'établissement d'une connexion
TcpTimeout	La connexion n'a pas pu être établie dans le délai imparti
ConnectionFunctionError	Une exception non détectée a été déclenchée lors de l'exécution de la fonction de connexion
Internal (Interne)	Une erreur de service interne s'est produite
UnmappedConnectionError	Une erreur s'est produite qui ne correspond à aucune des autres catégories

TLS mutuel d'origine avec CloudFront

L'authentification TLS mutuelle (Mutual Transport Layer Security Authentication — mTLS) est un protocole de sécurité qui étend l'authentification TLS standard en exigeant une authentification

bidirectionnelle basée sur des certificats, dans laquelle le client et le serveur doivent prouver leur identité avant d'établir une connexion sécurisée.

Viewer mTLS contre Origin mTLS

L'authentification mutuelle (mTL) peut être activée entre les spectateurs et votre CloudFront distribution (mTL des spectateurs), and/or ainsi qu'entre votre CloudFront distribution et l'origine (mTL d'origine). Cette documentation concerne la configuration mTLS d'origine. Pour la configuration mTLS du visualiseur, reportez-vous à :Authentification TLS mutuelle avec CloudFront (Viewer MTLS).

Origin mTLS permet CloudFront de s'authentifier auprès de vos serveurs d'origine à l'aide de certificats clients. Avec origin mTLS, vous pouvez vous assurer que seules vos CloudFront distributions autorisées peuvent établir des connexions avec vos serveurs d'applications, ce qui contribue à vous protéger contre les tentatives d'accès non autorisées.

> **Note**
>
> Dans les connexions mTLS d'origine, CloudFront agit en tant que client et présente son certificat client à votre serveur d'origine lors de la prise de contact TLS. CloudFront n'effectue pas de validation de la validité ou de l'état de révocation du certificat client. C'est la responsabilité de votre serveur d'origine. Votre infrastructure d'origine doit être configurée pour valider le certificat client par rapport à sa banque de confiance, vérifier l'expiration du certificat et effectuer des contrôles de révocation (tels que la validation CRL ou OCSP) conformément à vos exigences de sécurité. CloudFront le rôle se limite à la présentation du certificat ; toutes les logiques de validation des certificats et les politiques de sécurité sont appliquées par vos serveurs d'origine.

Comment ça marche

Dans un handshake TLS standard entre CloudFront et une origine, seul le serveur d'origine présente un certificat pour prouver son identité. CloudFront Avec les mTLS d'origine, le processus d'authentification devient bidirectionnel. Lorsque vous CloudFront tentez de vous connecter à votre serveur d'origine, CloudFront présente un certificat client lors de la prise de contact TLS. Votre serveur d'origine valide ce certificat auprès de sa banque de confiance avant d'établir la connexion sécurisée.

Cas d’utilisation

Origin mTLS répond à plusieurs scénarios de sécurité critiques dans lesquels les méthodes d'authentification traditionnelles entraînent une surcharge opérationnelle :

- Sécurité hybride et multicloud : vous pouvez sécuriser les connexions entre CloudFront et les origines hébergées en externe AWS ou les origines publiques sur AWS. Cela élimine le besoin de gérer des listes d'adresses IP autorisées ou des solutions d'en-tête personnalisées, fournissant une authentification cohérente basée sur des certificats entre AWS les centres de données sur site et les fournisseurs tiers. Les sociétés de médias, les détaillants et les entreprises exploitant une infrastructure distribuée bénéficient de contrôles de sécurité standardisés sur l'ensemble de leur infrastructure.
- Sécurité des API et du backend B2B : vous pouvez protéger vos API et microservices principaux contre les tentatives d'accès direct tout en préservant CloudFront les avantages en termes de performances. Les plateformes SaaS, les systèmes de traitement des paiements et les applications d'entreprise soumis à des exigences d'authentification strictes peuvent vérifier que les demandes d'API proviennent uniquement de CloudFront distributions autorisées, empêchant ainsi les attaques de type « man-in-the-middle » et les tentatives d'accès non autorisées.

Important : configuration requise pour le serveur Origin

Origin mTLS nécessite que vos serveurs d'origine soient configurés pour prendre en charge l'authentification TLS mutuelle. Votre infrastructure d'origine doit être capable de :

- Demande et validation de certificats clients lors des handshakes TLS
- Gestion d'un magasin de confiance avec les certificats de l'autorité de certification qui a émis les certificats CloudFront clients
- Enregistrement et surveillance des événements de connexion TLS mutuels
- Gestion des politiques de validation des certificats et gestion des échecs d'authentification

CloudFront gère la présentation des certificats côté client, mais vos serveurs d'origine sont chargés de valider ces certificats et de gérer la connexion TLS mutuelle. Assurez-vous que votre infrastructure d'origine est correctement configurée avant d'activer les mTL d'origine dans CloudFront.

Prise en main

Pour implémenter les mTLS d'origine avec CloudFront, vous devez importer le certificat client dans le Gestionnaire de AWS certificats, configurer votre serveur d'origine pour qu'il exige un TLS mutuel et activer les mTL d'origine sur votre distribution. CloudFront Les sections suivantes fournissent des instructions détaillées pour chaque tâche de configuration.

Rubriques

- Gestion des certificats avec AWS Gestionnaire de certificats
- Activer le protocole TLS mutuel d'origine pour les distributions CloudFront
- Utilisation de CloudFront fonctions avec un TLS mutuel d'origine

Gestion des certificats avec AWS Gestionnaire de certificats

AWS Le gestionnaire de certificats (ACM) stocke les certificats clients qui sont présentés à CloudFront vos serveurs d'origine lors de l'authentification TLS mutuelle d'origine.

Assistance aux autorités de certification

CloudFront origin mTLS nécessite des certificats clients avec utilisation étendue des clés (EKU) pour l'authentification client TLS. En raison de cette exigence, vous devez émettre des certificats auprès de votre autorité de certification et les importer dans AWS Certificate Manager. Les fonctionnalités de provisionnement et de renouvellement automatiques des certificats ACM ne sont pas disponibles pour les certificats clients mTLS d'origine. CloudFront origin mTLS prend en charge les certificats clients provenant de deux sources :

- AWS Autorité de certification privée : vous pouvez émettre des certificats depuis AWS une autorité de certification privée à l'aide de modèles de certificats qui incluent l'authentification du client TLS dans le champ Utilisation étendue des clés (tel que le EndEntityClientAuthCertificate modèle). Après avoir émis le certificat par AWS Private CA, vous devez l'importer dans ACM dans la région USA Est (Virginie du Nord) (us-east-1). Cette approche offre les avantages de sécurité d'une autorité de certification AWS privée tout en vous permettant de contrôler la gestion du cycle de vie des certificats.
- Third-party Autorités de certification privées : vous pouvez également émettre des certificats à partir de votre infrastructure d'autorité de certification privée existante et les importer dans ACM. Cela vous permet de maintenir vos processus actuels de gestion des certificats tout en tirant parti

des fonctionnalités mTLS CloudFront d'origine. Les certificats doivent inclure l'authentification du client TLS dans le champ Utilisation étendue des clés et doivent être au format PEM avec le certificat, la clé privée et la chaîne de certificats.

> **Important**
>
> Pour les autorités de certification AWS privées et les autorités de certification tierces, vous êtes responsable de la surveillance des dates d'expiration des certificats et de l'importation des certificats renouvelés dans ACM avant leur expiration. La fonction de renouvellement automatique d'ACM ne s'applique pas aux certificats importés utilisés pour les mTL d'origine.

Exigences et spécifications relatives aux certificats

Exigences relatives aux certificats clients

- Format : format PEM (Privacy Enhanced Mail)
- Composants : certificat, clé privée et chaîne de certificats
- Profondeur maximale de la chaîne de certificats : 3 (certificat feuille + certificat intermédiaire + certificat racine)
- Taille maximale de la chaîne de certificats : 64 Ko
- Taille du certificat : ne peut pas dépasser 96 Ko
- Taille maximale de la clé privée : 5 Ko (restriction ACM)
- Nombre maximum d'ARN de certificats mTLS d'origine unique pouvant être ajoutés ou modifiés par appel d'API de création ou de mise à jour de CloudFront distribution : 5
- Région : les certificats doivent être stockés dans ACM dans la région de l'est des États-Unis (Virginie du Nord) (us-east-1)

Spécifications des certificats pris en charge

- Type de certificat : X.509v3
- Algorithmes à clé publique :
  - RSA : 2 048 bits
  - ECDSA : P-256

- Algorithmes de signature :
  - SHA256, SHA384, SHA512 avec RSA
  - SHA256, SHA384, SHA512 avec ECDSA
  - SHA256, SHA384, SHA512 avec MGF1 RSASSA-PSS
- Utilisation étendue de la clé (obligatoire) : le certificat nécessite que l'extension Extended Key Usage (EKU) soit définie sur TLS Client Authentication, afin de s'assurer qu'elle est autorisée à des fins mTLS

Exigences relatives aux certificats de serveur

Vos serveurs d'origine doivent présenter des certificats provenant d'autorités de certification reconnues publiquement lors de la prise de contact TLS mutuelle. Pour plus de détails sur les exigences relatives aux certificats du serveur d'origine, consultez la section Exigences relatives à l'utilisation de SSL/TLS certificats avec CloudFront.

Demander ou importer un certificat

Avant d'activer les mTLS d'origine, vous devez disposer d'un certificat client dans ACM.

Demandez et importez un certificat depuis AWS Autorisation de certification privée

Prérequis :

- Une autorité de certification AWS privée configurée dans votre compte
- Autorisation d'émettre des certificats depuis AWS une autorité de certification privée
- Autorisation d'importer des certificats dans ACM
- Un modèle de certificat (ARN) adapté à votre cas d'utilisation `Extended key usage:TLS web client authentication`
- Installez OpenSSL, AWS CLI et jq (pour analyser le JSON).

Pour demander un certificat à la PCA et l'importer dans ACM (AWS CLI)

1. Définissez l'ARN de votre autorité de certification privée dans une variable pour faciliter la réutilisation.

```
PCA_ARN="arn:aws:acm-pca:region:account:certificate-authority/12345678..."
```

2. Utilisez OpenSSL pour générer une clé P-256 privée ECDSA (courbe prime256v1) et une demande de signature de certificat (CSR), en vous assurant que l'indicateur -nodes est utilisé pour conserver la clé privée non chiffrée, comme l'exige l'importation ACM.

```
openssl req -new -newkey ec -pkeyopt ec_paramgen_curve:prime256v1 -nodes \
    -keyout private.key \
    -out request.csr \
    -subj "/CN=client.example.com"
```

3. Soumettez le CSR à votre autorité de certification AWS privée pour émettre un certificat, qui renvoie l'ARN du certificat nouvellement émis.

```
CERT_ARN=$(aws acm-pca issue-certificate \
    --certificate-authority-arn "$PCA_ARN" \
    --csr fileb://request.csr \
    --signing-algorithm "SHA256WITHECDSA" \
    --validity Value=365,Type="DAYS" \
    --template-arn arn:aws:acm-pca:::template/EndEntityCertificate/V1 \
    --query 'CertificateArn' --output text)
```

4. Récupérez le bundle de certificats auprès de AWS PCA à l'aide de la commande get-certificate, qui renvoie à la fois le certificat feuille et la chaîne, puis utilisez jq pour les séparer en fichiers distincts.

```
# Retrieve the full certificate bundle in JSON format
aws acm-pca get-certificate \
    --certificate-authority-arn "$PCA_ARN" \
    --certificate-arn "$CERT_ARN" \
    --output json > full_cert.json

# Split into Leaf and Chain
jq -r '.Certificate' full_cert.json > leaf_cert.pem
jq -r '.CertificateChain' full_cert.json > cert_chain.pem
```

5. Importez la clé privée non chiffrée, le certificat feuille et la chaîne de certificats dans AWS ACM, en utilisant le protocole fileb ://pour gérer correctement les données des fichiers binaires dans l'interface de ligne de commande.

```
aws acm import-certificate \
    --certificate fileb://leaf_cert.pem \
    --private-key fileb://private.key \
```

```
    --certificate-chain fileb://cert_chain.pem \
    --region us-east-1 \
    --query 'CertificateArn' \
    --output text
```

Importer un certificat depuis une autorité de certification tierce

Prérequis :

- Un certificat, une clé privée non chiffrée et une chaîne de certificats provenant de votre autorité de certification au format PEM
- Le certificat doit inclure une utilisation étendue de la clé pour l'authentification du client TLS
- Autorisations d'importation de certificats dans ACM

Pour importer un certificat dans ACM (AWS CLI)

```
aws acm import-certificate \
  --certificate fileb://certificate.pem \
  --private-key fileb://private-key.pem \
  --certificate-chain fileb://certificate-chain.pem \
  --region us-east-1 \
  --query 'CertificateArn' \
  --output text
```

Étapes suivantes

Après avoir obtenu ou importé votre certificat client dans ACM, vous pouvez configurer votre serveur d'origine pour exiger une authentification TLS mutuelle et activer les mTLS d'origine sur votre distribution. CloudFront Pour obtenir des instructions sur l'activation des mTLS d'origine dans CloudFront, consultez la section suivante « Activer le TLS mutuel d'origine pour les CloudFront distributions ».

Activer le protocole TLS mutuel d'origine pour les distributions CloudFront

Après avoir obtenu un certificat client via AWS Certificate Manager et configuré votre serveur d'origine pour qu'il exige un TLS mutuel, vous pouvez activer les mTLS d'origine sur votre CloudFront distribution.

Prérequis et exigences

Avant d'activer les mTL d'origine sur une CloudFront distribution, assurez-vous de disposer des éléments suivants :

- Un certificat client stocké dans AWS Certificate Manager dans la région USA Est (Virginie du Nord) (us-east-1)
- Serveurs d'origine configurés pour exiger une authentification TLS mutuelle et valider les certificats clients
- Serveurs Origin présentant des certificats provenant d'autorités de certification reconnues par le public
- Autorisations pour modifier les CloudFront distributions
- Origin mTLS est uniquement disponible sur les forfaits Business, Premium ou Pay as you go.

> **Note**
>
> Les mTLS d'origine peuvent être configurés pour des origines personnalisées (y compris des origines hébergées à l'extérieur AWS) et des AWS origines qui prennent en charge le TLS mutuel, comme Application Load Balancer et API Gateway.

> **Important**
>
> Les CloudFront fonctionnalités suivantes ne sont pas prises en charge avec les mTL d'origine :
>
> - Trafic gRPC : le protocole gRPC n'est pas pris en charge pour les origines avec les mTLS d'origine activés
> - WebSocket connexions : WebSocket le protocole n'est pas pris en charge pour les origines avec les mTLS d'origine activés
> - Origines des VPC : les mTL d'origine ne peuvent pas être utilisés avec les origines des VPC
> - Déclencheurs de demande d'origine et de réponse d'origine avec Lambda @Edge : les fonctions Lambda @Edge dans les positions de demande d'origine et de réponse d'origine ne sont pas prises en charge avec les mTL d'origine

- PoPs intégrés : le mTLS d'origine n'est pas pris en charge pour les POP intégrés

Activer les mTLS d'origine

Per-origin la configuration vous permet de spécifier différents certificats clients pour différentes origines au sein d'une même distribution. Cette approche offre une flexibilité maximale lorsque vos origines ont des exigences d'authentification différentes.

Pour les nouvelles distributions (console)

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Créer une distribution
3. Sélectionnez un plan tarifaire : choisissez Business ou Premium ou Pay As You Go (Origin mTLS n'est pas disponible dans le forfait gratuit)
4. Dans la section Paramètres d'origine, choisissez Type d'origine comme autre
5. Dans la section Paramètres d'origine, choisissez Personnaliser les paramètres d'origine
6. Configurez votre première origine (nom de domaine, protocole, etc.)
7. Dans la configuration d'origine, recherchez mTLS
8. Activez mTLS
9. Pour le certificat client, sélectionnez votre certificat dans le Gestionnaire de AWS certificats
10. (Facultatif) Ajoutez des origines supplémentaires avec leurs propres configurations mTLS d'origine
11. Complétez les paramètres de distribution restants et choisissez Créer une distribution

Pour les distributions existantes (console)

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans la liste de distribution, sélectionnez la distribution que vous souhaitez modifier. (Remarque : assurez-vous que votre distribution est soumise à un plan tarifaire Pro, Premium ou Pay As You Go. Si ce n'est pas le cas, vous devez mettre à jour votre plan tarifaire avant d'activer Origin (mTLS).

3. Choisissez l'onglet Origins
4. Sélectionnez l'origine que vous souhaitez configurer et choisissez Modifier
5. Dans les paramètres d'origine, recherchez mTLS
6. Activez mTLS
7. Pour le certificat client, sélectionnez votre certificat dans le Gestionnaire de AWS certificats. (Remarque : seuls les certificats clients dont la propriété EKU (Extended Key Usage) est définie sur « Authentification du client TLS » seront répertoriés)
8. Choisissez Enregistrer les modifications
9. Répétez l'opération pour d'autres origines si nécessaire

Utilisation AWS INTERFACE DE LIGNE DE COMMANDE (CLI)

Pour la configuration par origine, spécifiez les paramètres mTLS d'origine dans la configuration de chaque origine :

```
{
  "Origins": {
    "Quantity": 2,
    "Items": [
      {
        "Id": "origin-1",
        "DomainName": "api.example.com",
        "CustomOriginConfig": {
          "HTTPSPort": 443,
          "OriginProtocolPolicy": "https-only"
        },
        "OriginMtlsConfig": {
          "ClientCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
cert-1"
        }
      },
      {
        "Id": "origin-2",
        "DomainName": "backend.example.com",
        "CustomOriginConfig": {
          "HTTPSPort": 443,
          "OriginProtocolPolicy": "https-only"
        },
        "OriginMtlsConfig": {
```

```
          "CertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/cert-2"
        }
      }
    ]
  }
}
```

> **Note**
>
> CloudFront ne fournira pas le certificat client si le serveur ne le demande pas, ce qui permet à la connexion de se dérouler normalement.

Étapes suivantes

Après avoir activé les mTL d'origine sur votre CloudFront distribution, vous pouvez surveiller les événements d'authentification à l'aide des journaux CloudFront d'accès.

Utilisation de CloudFront fonctions avec un TLS mutuel d'origine

CloudFront Functions fournit un traitement léger et sans serveur à la périphérie pour personnaliser la diffusion du contenu. Lorsque vous utilisez le TLS mutuel d'origine avec des CloudFront fonctions, il existe des comportements et des limites spécifiques à prendre en compte en ce qui concerne la sélection et la manipulation de l'origine.

CloudFront Fonctions et opérations prises en charge

CloudFront Les fonctions peuvent interagir avec m TLS-enabled origines de la manière suivante :

mettre à jour RequestOrigin ()

La fonction update RequestOrigin () prend en charge des modifications limitées lorsque vous travaillez avec m TLS-enabled origins :

- Basculer entre les origines mTLS d'origine : vous pouvez mettre à jour la demande pour l'acheminer vers une autre origine utilisant des mTL d'origine, à condition que les deux origines utilisent le même certificat client. Cela vous permet d'implémenter une logique de routage personnalisée tout en maintenant l'authentification TLS mutuelle. La commutation entre les origines utilisant différents certificats est prise en charge via les `createRequestOriginGroup()` API `selectRequestOriginById()` et.

- Désactivation des mTLS d'origine : vous pouvez passer d'une TLS-enabled origine m à une origine non MTLS en `mTLSConfig: 'off'` paramétrant la fonction. Cela permet de désactiver de manière conditionnelle l'authentification TLS mutuelle en fonction des caractéristiques de la demande.

Exemple : Basculer entre les origines mTLS d'origine avec le même certificat

```
import cf from 'cloudfront';

function handler(event) {
    var request = event.request;

    // Route to different origin based on request path
    if (request.uri.startsWith('/api/v2')) {
        cf.updateRequestOrigin({
            "domainName": "api-v2.example.com",
            "mTLSConfig": "inherit",
            // If no value is provided for mTLSConfig, it defaults to inherit
            // Both origins must use the same certificate
        });
    }

    return request;
}
```

Exemple : désactivation conditionnelle des mTL d'origine

```
import cf from 'cloudfront';

function handler(event) {
    var request = event.request;

    // Disable mTLS for specific paths
    if (request.uri.startsWith('/public')) {
        cf.updateRequestOrigin({
            "domainName": "public-origin.example.com",
            "mTLSConfig": "off"
        });
    }

    return request;
```

```
}
```

sélectionnez RequestOriginById ()

La `selectRequestOriginById()` fonction prend en charge la sélection d'origines pour lesquelles le TLS mutuel (origine) est activé. Vous pouvez utiliser cette fonction pour acheminer dynamiquement les demandes vers les TLS-enabled origines m configurées dans votre distribution. Lors de la sélection d'une origine par ID activée par TLS mutuel (origine), CloudFront utilise le certificat client configuré pour cette origine dans les paramètres de distribution.

Exemple : sélection d'une origine mutuelle activée par TLS (origine) par ID

```
import cf from 'cloudfront';

function handler(event) {
    var request = event.request;

    // Select mTLS-enabled origin based on request characteristics
    if (request.uri.startsWith('/secure-api')) {
        cf.selectRequestOriginById("mtls-origin-1");
    }

    return request;
}
```

créer RequestOriginGroup ()

La `createRequestOriginGroup()` fonction prend en charge la création de groupes d'origine qui incluent des origines mutuelles activées par TLS (origine). Vous pouvez créer dynamiquement des groupes d'origine avec m TLS-enabled origines pour les scénarios de basculement dans CloudFront Functions.

Exemple : création d'un groupe d'origine avec des origines mutuelles activées par le protocole TLS (origine)

```
import cf from 'cloudfront';

function handler(event) {
    // Create origin group with mTLS-enabled primary and failover origins
    cf.createRequestOriginGroup({
        "originIds": ["mtls-origin-primary", "mtls-origin-failover"],
        "failoverCriteria": {
```

```
            "statusCodes": [500, 502, 503, 504]
        }
    });

    return event.request;
}
```

Offre de contenu privé avec des URL et des cookies signés

De nombreuses entreprises qui distribuent du contenu via Internet veulent limiter l'accès aux documents, données professionnelles, flux multimédias ou contenus destinés à des utilisateurs sélectionnés, tels que ceux qui paient un droit. Pour diffuser ce contenu privé en toute sécurité à l'aide de CloudFront, vous pouvez effectuer les opérations suivantes :

- Exigez que vos utilisateurs accèdent à votre contenu privé en utilisant des URL spéciales CloudFront signées ou des cookies signés.
- Exigez que vos utilisateurs accèdent à votre contenu en utilisant CloudFront des URL, et non des URL qui accèdent au contenu directement sur le serveur d'origine (par exemple, Amazon S3 ou un serveur HTTP privé). Il n'est pas nécessaire d'exiger des CloudFront URL, mais nous le recommandons pour empêcher les utilisateurs de contourner les restrictions que vous spécifiez dans les URL signées ou les cookies signés.

Pour plus d'informations, consultez Restriction de l'accès aux fichiers.

Comment diffuser du contenu privé

CloudFront Pour configurer la diffusion de contenu privé, effectuez les tâches suivantes :

1. (Facultatif mais recommandé) Demandez à vos utilisateurs d'accéder à votre contenu uniquement via CloudFront. La méthode que vos utilisez varie selon que vous recourez aux origines Amazon S3 ou aux origines personnalisées :

   - Amazon S3 : voir the section called "Restriction de l'accès à une origine Amazon S3".
   - Origine personnalisée : voir Restriction de l'accès à des fichiers d'origines personnalisées.

   Les origines personnalisées incluent Amazon EC2, les compartiments Amazon S3 configurés en tant que points de terminaison de site Web, Elastic Load Balancing et vos propres serveurs web HTTP.

2. Spécifiez les groupes de clés approuvés ou les signataires approuvés que vous souhaitez utiliser pour créer des URL ou des cookies signés. Nous vous recommandons d'utiliser des groupes de clés approuvés. Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.
3. Écrivez votre application pour répondre aux demandes des utilisateurs authentifiés avec des URL signées ou avec des en-têtes `Set-Cookie` définissant des cookies signés. Suivez les étapes décrites dans l'une des rubriques suivantes :

   - Utilisation des URL signées
   - Utilisation de cookies signés

   En cas de doute sur la méthode à utiliser, consultez Choix entre des URL signées et des cookies signés.

Rubriques

- Restriction de l'accès aux fichiers
- Spécification des signataires qui peuvent créer des URL et des cookies signés
- Choix entre des URL signées et des cookies signés
- Utilisation des URL signées
- Utilisation de cookies signés
- Utilisation d'une commande Linux et OpenSSL pour le chiffrement et l'encodage en base64
- Exemples de code pour la création de la signature d'une URL signée

Restriction de l'accès aux fichiers

Vous pouvez contrôler l'accès des utilisateurs à votre contenu privé de deux façons :

- Restreignez l'accès aux fichiers contenus dans les CloudFront caches.
- Restreignez l'accès aux fichiers dans votre origine en effectuant l'une des actions suivantes :
  - Configurez un contrôle d'accès à l'origine (OAC) pour votre compartiment Amazon S3.
  - Configurez des en-têtes personnalisés pour un serveur HTTP privé (origine personnalisée).

Restreindre l'accès aux fichiers dans les CloudFront caches

Vous pouvez configurer CloudFront pour exiger que les utilisateurs accèdent à vos fichiers à l'aide d'URL signées ou de cookies signés. Vous pouvez alors développer votre application pour créer et distribuer des URL signées aux utilisateurs authentifiées ou pour envoyer des en-têtes `Set-Cookie` qui définissent des cookies signés pour des utilisateurs authentifiés. (Pour fournir à quelques utilisateurs un accès à long terme à un petit nombre de fichiers, vous pouvez aussi créer des URL signées manuellement.)

Lorsque vous créez des URL signées ou des cookies signés pour contrôler l'accès à vos fichiers, vous pouvez spécifier les restrictions suivantes :

- Une heure et une date de fin, au-delà desquelles l'URL n'est plus valide.
- (Facultatif) L'heure et la date auxquelles l'URL devient valide.
- (Facultatif) L'adresse IP ou la plage d'adresses IP des ordinateurs qui peuvent être utilisés pour accéder à votre contenu.

Une partie d'une URL signée ou d'un cookie signé est hachée et signée à l'aide de la clé privée d'une paire de clés publique/privée. Lorsqu'une personne utilise une URL signée ou un cookie signé pour accéder à un fichier, CloudFront compare les parties signées et non signées de l'URL ou du cookie. S'ils ne correspondent pas, le fichier CloudFront ne sera pas diffusé.

Vous devez utiliser les clés privées RSA 2048 ou ECDSA 256 pour signer les URL ou les cookies.

Restriction de l'accès aux fichiers dans les compartiments Amazon S3

Vous pouvez éventuellement sécuriser le contenu de votre compartiment Amazon S3 afin que les utilisateurs puissent y accéder via la CloudFront distribution spécifiée mais ne puissent pas y accéder directement à l'aide des URL Amazon S3. Cela empêche quiconque de contourner CloudFront et d'utiliser l'URL Amazon S3 pour accéder au contenu auquel vous souhaitez restreindre l'accès. Cette étape n'est pas obligatoire pour utiliser les URL signées, mais nous la recommandons.

Pour obliger les utilisateurs à accéder à votre contenu via CloudFront des URL, vous devez effectuer les tâches suivantes :

- Autorisez un contrôle CloudFront d'accès à l'origine à lire les fichiers du compartiment S3.
- Créez le contrôle d'accès à l'origine et associez-le à votre CloudFront distribution.

- Supprimez l’autorisation pour toute autre personne d’utiliser les URL Amazon S3 pour lire les fichiers.

Pour plus d’informations, consultez the section called “Restriction de l’accès à une origine Amazon S3” ou the section called “Restreindre l'accès à l'origine d'un point Multi-Region d'accès Amazon S3”.

Restriction de l’accès à des fichiers d’origines personnalisées

Si vous utilisez une origine personnalisée, vous pouvez éventuellement configurer des en-têtes personnalisés pour limiter l’accès. CloudFront Pour obtenir vos fichiers à partir d'une origine personnalisée, les fichiers doivent être accessibles à l'CloudFront aide d'une requête HTTP (ou HTTPS) standard. Mais en utilisant des en-têtes personnalisés, vous pouvez restreindre davantage l'accès à votre contenu afin que les utilisateurs puissent y accéder uniquement viaCloudFront, et non directement. Cette étape n’est pas obligatoire pour utiliser les URL signées, mais nous la recommandons.

Pour obliger les utilisateurs à accéder au contenu via CloudFront, modifiez les paramètres suivants dans vos CloudFront distributions :

Origin Custom Headers

: Configurez CloudFront pour transférer les en-têtes personnalisés vers votre origine. Consultez Configurer CloudFront pour ajouter des en-têtes personnalisés aux demandes d'origine.

Viewer Protocol Policy

: Configurez votre distribution de manière à ce que les utilisateurs emploient HTTPS pour accéder à CloudFront. Consultez Viewer Protocol Policy.

Origin Protocol Policy

: Configurez votre distribution de manière CloudFront à exiger l'utilisation du même protocole que les spectateurs pour transmettre les demandes à l'origine. Consultez Protocole (origines personnalisées uniquement).

Après avoir effectué ces modifications, mettez à jour votre application en fonction de votre origine personnalisée afin d'accepter uniquement les demandes qui incluent les en-têtes personnalisés que vous avez configurés CloudFront pour envoyer.

La combinaison de la politique du protocole Viewer et de la politique du protocole d'origine garantit que les en-têtes personnalisés sont chiffrés en transit. Cependant, nous vous recommandons d'effectuer régulièrement les opérations suivantes pour faire pivoter les en-têtes personnalisés qui sont CloudFront redirigés vers votre origine :

1. Mettez à jour votre CloudFront distribution pour commencer à transférer un nouvel en-tête vers votre origine personnalisée.
2. Mettez à jour votre application pour accepter le nouvel en-tête comme confirmation de l'origine de la demande CloudFront.
3. Lorsque les demandes n'incluent plus l'en-tête que vous remplacez, mettez à jour votre application pour ne plus accepter l'ancien en-tête comme confirmation de l'origine de la demande CloudFront.

Spécification des signataires qui peuvent créer des URL et des cookies signés

Rubriques

- Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS
- Création de paires de clés pour vos signataires
- Reformatage de la clé privée (.NET et Java uniquement)
- Ajout d’un signataire à une distribution
- Rotation de paires de clés

Pour créer des URL ou des cookies signés, vous avez besoin d’un signataire. Un signataire est soit un groupe de clés de confiance dans lequel vous créez CloudFront, soit un AWS compte contenant une paire de CloudFront clés. Nous vous recommandons d’utiliser des groupes de clés approuvés avec des URL et des cookies signés. Pour plus d’informations, consultez Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS.

Le signataire a deux finalités :

- Dès que vous ajoutez le signataire à votre distribution, CloudFront les spectateurs doivent utiliser des URL signées ou des cookies signés pour accéder à vos fichiers.
- Lorsque vous créez des URL ou des cookies signés, vous utilisez la clé privée de la paire de clés du signataire pour signer une partie de l’URL ou du cookie. Lorsque quelqu'un demande un fichier restreint, CloudFront compare la signature de l'URL ou du cookie avec l'URL ou le cookie non

signé pour vérifier qu'il n'a pas été falsifié. CloudFront vérifie également que l'URL ou le cookie est valide, ce qui signifie, par exemple, que la date et l'heure d'expiration ne sont pas dépassées.

Lorsque vous spécifiez un signataire, vous spécifiez également indirectement les fichiers qui requièrent des URL ou des cookies signés en ajoutant le signataire à un comportement de cache. Si votre distribution ne comporte qu'un seul comportement de cache, les utilisateurs doivent employer des URL ou des cookies signés pour accéder à un fichier de la distribution. Si vous créez plusieurs comportements de cache et que vous ajoutez des utilisateurs à certains comportements de cache et pas à d'autres, vous pouvez exiger que les utilisateurs emploient des URL ou des cookies signés pour accéder à certains fichiers, et non à d'autres.

Pour spécifier les signataires (les clés privées) autorisés à créer des URL signées ou des cookies signés, et pour ajouter les signataires à votre CloudFront distribution, effectuez les tâches suivantes :

1. Décidez si vous souhaitez utiliser un groupe de clés sécurisé ou un Compte AWS en tant que signataire. Nous vous recommandons d'utiliser un groupe de clés approuvé. Pour plus d'informations, consultez Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS.
2. Pour le signataire que vous avez choisi à l'étape 1, créez une paire de clés privées/publiques. Pour plus d'informations, consultez Création de paires de clés pour vos signataires.
3. Si vous utilisez .NET ou Java pour créer des URL signées ou des cookies signés, reformatez la clé privée. Pour plus d'informations, consultez Reformatage de la clé privée (.NET et Java uniquement).
4. Dans la distribution pour laquelle vous créez des URL ou des cookies signés, spécifiez le signataire. Pour plus d'informations, consultez Ajout d'un signataire à une distribution.

Choisissez entre des groupes de clés fiables (recommandé) et Comptes AWS

Pour utiliser des URL ou des cookies signés, vous avez besoin d'un signataire. Un signataire est soit un groupe de clés fiables dans lequel vous créez CloudFront, soit un groupe Compte AWS qui contient une paire de CloudFront clés. Nous vous recommandons d'utiliser des groupes de clés approuvés, pour les raisons suivantes :

- Avec les groupes de CloudFront clés, vous n'avez pas besoin d'utiliser l'utilisateur root du AWS compte pour gérer les clés publiques des URL CloudFront signées et des cookies signés. AWS les meilleures pratiques recommandent de ne pas utiliser l'utilisateur root lorsque ce n'est pas nécessaire.

- CloudFront Les groupes de clés vous permettent de gérer les clés publiques, les groupes de clés et les signataires de confiance à l'aide de l' CloudFront API. Vous pouvez utiliser l'API pour automatiser la création et la rotation des clés. Lorsque vous utilisez l'utilisateur AWS root, vous devez utiliser Console de gestion AWS pour gérer les paires de CloudFront clés, vous ne pouvez donc pas automatiser le processus.
- Comme vous pouvez gérer des groupes de clés à l'aide de l' CloudFront API, vous pouvez également utiliser des politiques d'autorisations Gestion des identités et des accès AWS (IAM) pour limiter ce que les différents utilisateurs sont autorisés à faire. Par exemple, vous pouvez autoriser les utilisateurs à télécharger des clés publiques, mais pas à les supprimer. Vous pouvez également autoriser les utilisateurs à supprimer des clés publiques, mais uniquement lorsque certaines conditions sont remplies, telles que l'utilisation d'une authentification à plusieurs facteurs, l'envoi de la demande à partir d'un réseau particulier ou dans une plage de dates et d'heures spécifiques.
- Grâce aux groupes de CloudFront clés, vous pouvez associer un plus grand nombre de clés publiques à votre CloudFront distribution, ce qui vous donne plus de flexibilité dans la manière dont vous utilisez et gérez les clés publiques. Par défaut, vous pouvez associer jusqu'à quatre groupes de clés avec une seule distribution, et vous pouvez avoir jusqu'à cinq clés publiques dans un groupe de clés.

  Lorsque vous utilisez l'utilisateur root du AWS compte pour gérer les paires de CloudFront clés, vous ne pouvez avoir que deux paires de CloudFront clés actives par AWS compte.

Création de paires de clés pour vos signataires

Chaque signataire que vous utilisez pour créer des URL CloudFront signées ou des cookies signés doit disposer d'une paire de clés publique-privée. Le signataire utilise sa clé privée pour signer l'URL ou les cookies, et CloudFront utilise la clé publique pour vérifier la signature.

La manière dont vous créez une paire de clés varie selon que vous utilisez un groupe de clés sécurisé comme signataire (recommandé) ou une paire de CloudFront clés. Pour plus d'informations, consultez les sections suivantes. La paire de clés que vous créez doit satisfaire aux exigences suivantes :

- Il doit s'agir d'une paire de SSH-2 clés RSA 2048 ou ECDSA 256.
- Elle doit être au format PEM codé en base64.

Pour aider à sécuriser vos applications, nous vous recommandons d'effectuer une rotation périodique des paires de clés. Pour plus d'informations, consultez Rotation de paires de clés.

Création d'une paire de clés pour un groupe de clés approuvé (recommandé)

Pour créer une paire de clés pour un groupe de clés approuvé, effectuez les opérations suivantes :

1. Créez la paire de clés privées/publiques.
2. Téléchargez la clé publique sur CloudFront.
3. Ajoutez la clé publique à un groupe de CloudFront clés.

Pour plus d'informations, consultez les procédures suivantes.

Pour créer une paire de clés

> **Note**
>
> Les étapes suivantes utilisent OpenSSL comme exemple d'une méthode permettant de créer une paire de clés. Il existe de nombreuses autres façons de créer une paire de clés RSA ou ECDSA.

1. Exécutez une des commandes d'exemple suivantes :

   - L'exemple de commande suivant utilise OpenSSL pour générer une paire de clés RSA d'une longueur de 2048 bits et l'enregistrer dans le fichier nommé `private_key.pem`.

     ```
     openssl genrsa -out private_key.pem 2048
     ```

   - L'exemple de commande suivant utilise OpenSSL pour générer une paire de clés ECDSA avec la courbe `prime256v1` et l'enregistrer dans le fichier nommé `private_key.pem`.

     ```
     openssl ecparam -name prime256v1 -genkey -noout -out privatekey.pem
     ```

2. Le fichier obtenu contient à la fois la clé publique et la clé privée. L'exemple de commande suivant extrait la clé publique du fichier nommé `private_key.pem`.

   ```
   openssl rsa -pubout -in private_key.pem -out public_key.pem
   ```

Vous chargez la clé publique (dans le fichier `public_key.pem`) ultérieurement, dans le cadre de la procédure suivante.

Pour télécharger la clé publique sur CloudFront

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le menu de navigation, choisissez Clés publiques.
3. Choisissez Créer une clé publique.
4. Dans la fenêtre Créer une clé publique procédez comme suit :

   a. Dans Nom de la clé, saisissez un nom pour identifier la clé publique.

   b. Dans Valeur de clé, collez la clé publique. Si vous avez suivi les étapes de la procédure précédente, la clé publique se trouve dans le fichier nommé `public_key.pem`. Pour copier et coller le contenu de la clé publique, vous pouvez :

      - Utilisez la commande cat sur la ligne de commande macOS ou Linux, comme ceci :

        ```
        cat public_key.pem
        ```

        Copiez la sortie de cette commande, puis collez-la dans le champ Valeur de clé.
      - Ouvrez le `public_key.pem` fichier à l'aide d'un éditeur de texte brut tel que Notepad (sous Windows) ou TextEdit (sous macOS). Copiez le contenu du fichier, puis collez-le dans le champ Valeur de clé.

   c. (Facultatif) Dans Commentaire, ajoutez un commentaire pour décrire la clé publique.

   Lorsque vous avez terminé, choisissez Ajouter.
5. Enregistrez l'ID de clé publique. Vous l'utiliserez ultérieurement lors de la création des URL ou des cookies signés, comme valeur du champ `Key-Pair-Id`.

Pour ajouter la clé publique à un groupe de clés

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le menu de navigation, choisissez Groupes de clés.

3. Choisissez Ajouter un groupe de clés.
4. Sur la page Créer un groupe de clés procédez comme suit :
   a. Dans Nom du groupe de clés, saisissez un nom pour identifier le groupe de clés.
   b. (Facultatif) Dans Commentaire, saisissez un commentaire pour décrire le groupe de clés.
   c. Dans Clés publiques, sélectionnez la clé publique à ajouter au groupe de clés, puis choisissez Ajouter. Répétez cette étape pour chaque clé publique que vous souhaitez ajouter au groupe de clés.
5. Choisissez Créer une paire de clés.
6. Enregistrez le nom du groupe de clés. Vous l'utiliserez ultérieurement pour associer le groupe de clés à un comportement de cache dans une CloudFront distribution. (Dans l' CloudFront API, vous utilisez l'ID du groupe de clés pour associer le groupe de clés à un comportement de cache.)

Créez une paire de CloudFront clés (non recommandé, nécessite le Compte AWS utilisateur root)

> **Important**
>
> Nous vous recommandons de créer une clé publique pour un groupe de clés approuvé au lieu de suivre ces étapes. Pour connaître la manière recommandée de créer des clés publiques pour les URL signées et les cookies signés, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).

Vous pouvez créer une paire de CloudFront clés de la manière suivante :

- Créez une paire de clés dans le Console de gestion AWS et téléchargez la clé privée. Consultez la procédure suivante.
- Créez une paire de clés RSA à l'aide d'une application tel qu'OpenSSL, puis chargez la clé publique sur Console de gestion AWS. Pour plus d'informations sur la création d'une paire de clés, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).

Pour créer des paires de CloudFront clés dans Console de gestion AWS

1. Connectez-vous à l' Console de gestion AWS aide des informations d'identification de l'utilisateur root du AWS compte.

> **Important**
>
> Les utilisateurs IAM ne peuvent pas créer de paires de CloudFront clés. Pour créer des paires de clés, vous devez vous connecter à l'aide des informations d'identification de l'utilisateur racine.

2. Choisissez le nom de votre compte, puis Mes informations d'identification de sécurité.
3. Choisissez CloudFront des paires de clés.
4. Confirmez que vous n'avez pas plus d'une paire de clés active. Vous ne pouvez pas créer une paire de clés si vous en avez déjà deux actives.
5. Choisissez Créer une nouvelle paire de clés.

> **Note**
>
> Vous pouvez également choisir de créer votre propre paire de clés et de télécharger la clé publique. CloudFront les paires de clés prennent en charge les clés de 1024, 2048 ou 4096 bits.

6. Dans la boîte de dialogue Créer une paire de clés, choisissez Télécharger fichier de clés privées, puis enregistrez le fichier sur votre ordinateur.

> **Important**
>
> Enregistrez la clé privée de votre paire de CloudFront clés dans un emplacement sécurisé et définissez des autorisations sur le fichier de manière à ce que vous soyez le seul à pouvoir le lire. Si quelqu'un obtient votre clé privée, il peut générer des cookies signés et des URL signées valides, et télécharger votre contenu. Vous ne pouvez pas récupérer la clé privée. Par conséquent, si vous la perdez ou la supprimez, vous devez créer une nouvelle paire de CloudFront clés.

7. Enregistrez l'ID de paire de clés de votre paire de clés. (Dans le Console de gestion AWS, cela s'appelle l'ID de clé d'accès.) Vous l'utiliserez quand vous créerez des cookies ou des URL signés.

Reformatage de la clé privée (.NET et Java uniquement)

Si vous utilisez .NET ou Java pour créer des URL signées ou des cookies signés, vous ne pouvez pas utiliser la clé privée de votre paire de clés au format PEM par défaut pour créer la signature. Dans ce cas, procédez comme suit :

- .NET framework : convertit la clé privée au format XML utilisé par .NET framework. Plusieurs outils sont disponibles.
- Java : convertit la clé privée au format DER. On peut utiliser la commande OpenSSL suivante pour le faire. Dans la commande suivante, `private_key.pem` se trouve le nom du fichier contenant la clé PEM-formatted privée et `private_key.der` le nom du fichier contenant la clé DER-formatted privée après avoir exécuté la commande.

  ```
  openssl pkcs8 -topk8 -nocrypt -in private_key.pem -inform PEM -out private_key.der -
  outform DER
  ```

  Pour vous assurer que l'encodeur fonctionne correctement, ajoutez le JAR des API de cryptographie Java de Bouncy Castle à votre projet, puis ajoutez le fournisseur Bouncy Castle.

Ajout d’un signataire à une distribution

Un signataire est le groupe de clés de confiance (recommandé) ou la paire de CloudFront clés qui peut créer des URL signées et des cookies signés pour une distribution. Pour utiliser des URL signées ou des cookies signés avec une CloudFront distribution, vous devez spécifier un signataire.

Les signataires sont associés aux comportements de cache. Vous pouvez ainsi exiger des URL signées ou des cookies signés pour certains fichiers et pas pour d'autres de la même distribution. Une distribution nécessite des URL ou des cookies signés uniquement pour les fichiers associés aux comportements de cache correspondants.

De même, un signataire peut uniquement signer des URL ou des cookies pour les fichiers associés aux comportements de cache correspondants. Par exemple, si vous avez un signataire pour un comportement de cache et un autre pour un autre comportement de cache, ni l’un ni l’autre ne peuvent créer des URL ou des cookies signés pour les fichiers associés à l’autre comportement de cache.

Important

Avant d'ajouter un signataire à votre distribution, procédez comme suit :

- Définissez soigneusement les modèles de chemin d'accès dans les comportements de cache et la séquence des comportements de cache de façon à ne pas donner aux utilisateurs un accès non prévu à votre contenu ou à les empêcher d'accéder à un contenu que vous voulez disponible pour tout le monde.

  Par exemple, imaginons qu'une demande corresponde au modèle de chemin de deux comportements de cache. Le premier comportement de cache n'exige pas d'URL signées ou de cookies signés, à l'inverse du second comportement de cache. Les utilisateurs pourront accéder aux fichiers sans utiliser les URL signées ou les cookies signés, parce que CloudFront traite le comportement de cache associé à la première correspondance.

  Pour plus d'informations sur les modèles de chemin d'accès, consultez Modèle de chemin.
- Pour une distribution que vous utilisez déjà pour distribuer du contenu, assurez-vous d'être prêt à démarrer la génération d'URL et de cookies signés avant d'ajouter un signataire. Lorsque vous ajoutez un signataire, CloudFront rejette les demandes qui n'incluent pas d'URL signée ou de cookie signé valide.

Vous pouvez ajouter des signataires à votre distribution à l'aide de la CloudFront console ou de l' CloudFrontAPI.

Console

Les étapes suivantes montrent comment ajouter un groupe de clés approuvé en tant que signataire. Vous pouvez également ajouter un Compte AWS en tant que signataire de confiance, mais cela n'est pas recommandé.

Pour ajouter un signataire à une distribution à l'aide de la console

1. Enregistrez l'ID de groupe de clés du groupe de clés que vous souhaitez utiliser en tant que signataire approuvé. Pour plus d'informations, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).
2. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

3. Choisissez la distribution dont vous souhaitez protéger les fichiers avec des URL ou des cookies signés.

> **Note**
>
> Pour ajouter un signataire à une nouvelle distribution, vous spécifiez les mêmes paramètres que ceux décrits à l'étape 6 lors de la création de la distribution.

4. Choisissez l'onglet Comportements.
5. Sélectionnez le comportement du cache dont le modèle de chemin d'accès correspond aux fichiers que vous souhaitez protéger avec des URL ou des cookies signés, puis choisissez Modifier.
6. Sur la page Modifier le comportement procédez comme suit :
   a. Pour Restrict Viewer Access (Use Signed URLs or Signed Cookies), cliquez sur Yes.
   b. Dans Groupes de clés approuvés ou Signataire approuvé, choisissez Groupes de clés approuvés.
   c. Dans Groupes de clés approuvés, choisissez le groupe de clés à ajouter, puis Ajouter. Recommencez si vous souhaitez ajouter plusieurs groupes de clés.
7. Choisissez Oui, Modifier pour mettre à jour le comportement du cache.

API

Vous pouvez utiliser l' CloudFront API pour ajouter un groupe de clés de confiance en tant que signataire. Vous pouvez ajouter un signataire à une distribution existante ou à une nouvelle distribution. Dans les deux cas, spécifiez les valeurs dans l'élément `TrustedKeyGroups`.

Vous pouvez également ajouter un Compte AWS en tant que signataire de confiance, mais cela n'est pas recommandé.

Consultez les rubriques suivantes dans le manuel Amazon CloudFront API Reference :

- Mettre à jour une distribution existante — UpdateDistribution
- Créez une nouvelle distribution — CreateDistribution

Rotation de paires de clés

Nous vous recommandons d'effectuer une rotation (modifier) périodique de vos paires de clés pour les URL et les cookies signés. Pour effectuer une rotation des paires de clés que vous utilisez pour créer des URL ou des cookies signés sans invalider les URL ou cookies qui n'ont pas encore expiré, exécutez les tâches suivantes :

1. Créez une nouvelle paire de clés et ajoutez la clé publique à un groupe de clés. Pour plus d'informations, consultez Création d'une paire de clés pour un groupe de clés approuvé (recommandé).
2. Si vous avez créé un nouveau groupe de clés à l'étape précédente, ajoutez le groupe de clés à la distribution en tant que signataire.

   > **Important**
   >
   > Ne supprimez pas encore des clés publiques existantes du groupe de clés, ni les groupes de clés de la distribution. Ajoutez seulement les nouveaux.

3. Mettez à jour votre application pour créer des signatures à l'aide des clés privées à partir de la nouvelle paire de clés. Vérifiez que les URL ou les cookies signés avec les nouvelles clés privées fonctionnent.
4. Attendez jusqu'à ce que la date d'expiration soit passée dans les URL ou cookies signés à l'aide de la paire de clés précédente. Ensuite, supprimez l'ancienne clé publique du groupe de clés. Si vous avez créé un nouveau groupe de clés à l'étape 2, supprimez l'ancien groupe de clés de votre distribution.

Choix entre des URL signées et des cookies signés

CloudFront Les URL signées et les cookies signés fournissent les mêmes fonctionnalités de base : ils vous permettent de contrôler qui peut accéder à votre contenu. Si vous souhaitez diffuser du contenu privé CloudFront et que vous essayez de décider d'utiliser des URL signées ou des cookies signés, tenez compte des points suivants.

Utilisez les URL signées dans les cas suivants :

- Vous voulez restreindre l'accès aux fichiers individuels : par exemple, un téléchargement d'installation de votre application.

- Vos utilisateurs utilisent un client (par exemple, un client HTTP personnalisé) qui ne prend pas en charge les cookies.

Utilisez les cookies signés dans les cas suivants :

- Vous voulez fournir l'accès à plusieurs fichiers restreints : par exemple, tous les fichiers d'une vidéo au format HLS ou tous les fichiers de la section des abonnés d'un site web.
- Vous ne voulez pas modifier vos URL actuelles.

Si vous n'utilisez pas actuellement d'URL signées et si vos URL (non signées) contiennent l'un des paramètres de chaîne de requête suivants, vous ne pouvez pas utiliser d'URL signées ni de cookies signés :

- `Expires`
- `Policy`
- `Signature`
- `Key-Pair-Id`
- `Hash-Algorithm`

CloudFront suppose que les URL contenant l'un de ces paramètres de chaîne de requête sont des URL signées et ne seront donc pas considérées comme des cookies signés.

Utilisation des URL et des cookies signés

Les URL signées ont priorité sur les cookies signés. Si vous utilisez à la fois des URL signées et des cookies signés pour contrôler l'accès aux mêmes fichiers et qu'un utilisateur utilise une URL signée pour demander un fichier, CloudFront détermine s'il convient de renvoyer le fichier au visualiseur en se basant uniquement sur l'URL signée.

Utilisation des URL signées

Une URL signée inclut des informations supplémentaires, par exemple une heure et date d'expiration, qui vous donnent un meilleur contrôle de l'accès à votre contenu. Ces informations supplémentaires apparaissent dans une déclaration de politique, basée sur une politique prédéfinie ou une politique personnalisée. Les différences entre les politiques prédéfinies et les politiques personnalisées sont expliquées dans les deux prochaines sections.

> **Note**
>
> Vous pouvez créer certaines URL signées à l'aide de politiques prédéfinies et d'autres à l'aide de politiques personnalisées pour la même distribution.

Rubriques

- Choix entre des politiques prédéfinies et personnalisées pour les URL signées
- Fonctionnement des URL signées
- Choix de la durée de validité des URL signées
- Quand CloudFront vérifie la date et l'heure d'expiration dans une URL signée
- Exemple de code et outils tiers
- Création d'une URL signée à l'aide d'une politique prédéfinie
- Création d'une URL signée utilisant une politique personnalisée

Choix entre des politiques prédéfinies et personnalisées pour les URL signées

Lorsque vous créez une URL signée, vous écrivez une instruction de politique au format JSON qui spécifie les restrictions sur l'URL signée : par exemple, la durée de validité de l'URL. Vous pouvez utiliser une politique prédéfinie ou une politique personnalisée. Comparaison des politiques prédéfinies et des politiques personnalisées :

Description	Politique prédéfinie	Politique personnalisée
Vous pouvez réutiliser la déclaration de politique pour plusieurs fichiers. Pour ce faire, vous devez utiliser les caractères génériques de l'objet `Resource`. Pour plus d'informations, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée.)	Non	Oui

Description	Politique prédéfinie	Politique personnalisée
Vous pouvez indiquer la date et l'heure auxquelles les utilisateurs peuvent commencer à accéder à votre contenu.	Non	Oui (facultatif)
Vous pouvez indiquer la date et l'heure auxquelles les utilisateurs ne peuvent plus accéder à votre contenu.	Oui	Oui
Vous pouvez spécifier l'adresse IP ou la plage d'adresses IP des utilisateurs qui peuvent accéder à votre contenu.	Non	Oui (facultatif)
L'URL signée inclut une version encodée base 64 de la politique, ce qui se traduit par une URL plus longue.	Non	Oui

Pour plus d'informations sur la création d'URL signées à l'aide d'une politique prédéfinie, consultez Création d'une URL signée à l'aide d'une politique prédéfinie.

Pour plus d'informations sur la création d'URL signées à l'aide d'une politique personnalisée, consultez Création d'une URL signée utilisant une politique personnalisée.

Fonctionnement des URL signées

Voici un aperçu de la façon dont vous configurez CloudFront Amazon S3 pour les URL signées et de la façon dont il CloudFront répond lorsqu'un utilisateur utilise une URL signée pour demander un fichier.

1. Dans votre CloudFront distribution, spécifiez un ou plusieurs groupes de clés fiables, qui contiennent les clés publiques que CloudFront vous pouvez utiliser pour vérifier la signature de l'URL. Vous utilisez les clés privées correspondantes pour signer les URL.

   CloudFront prend en charge les URL signées avec des signatures de clé RSA 2048 et ECDSA 256.

Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.

2. Développez votre application pour déterminer si un utilisateur doit avoir accès à votre contenu et pour créer des URL signées pour les fichiers ou parties de votre application auxquels vous voulez limiter l'accès. Pour plus d'informations, consultez les rubriques suivantes :

   - Création d'une URL signée à l'aide d'une politique prédéfinie
   - Création d'une URL signée utilisant une politique personnalisée

3. Un utilisateur demande un fichier pour lequel vous voulez requérir des URL signées.
4. Votre application vérifie que l'utilisateur est autorisé à accéder au fichier : il est abonné, il a payé pour accéder au contenu ou il a satisfait à quelque autre condition pour accéder.
5. Votre application crée et renvoie une URL signée à l'utilisateur.
6. L'URL signée autorise l'utilisateur à télécharger ou diffuser le contenu.

   Cette étape est automatique ; l'utilisateur n'a généralement rien à faire de plus pour accéder au contenu. Pa exemple, si un utilisateur accède à votre contenu dans un navigateur web, votre application renvoie l'URL signée au navigateur. Le navigateur utilise immédiatement l'URL signée pour accéder au fichier dans le cache CloudFront périphérique sans aucune intervention de la part de l'utilisateur.
7. CloudFront utilise la clé publique pour valider la signature et confirmer que l'URL n'a pas été falsifiée. Si la signature n'est pas valide, la demande est rejetée.

   Si la signature est valide, CloudFront examine la déclaration de politique contenue dans l'URL (ou en crée une si vous utilisez une politique prédéfinie) pour confirmer que la demande est toujours valide. Par exemple, si vous avez spécifié une date et une heure de début et de fin pour l'URL, cela CloudFront confirme que l'utilisateur essaie d'accéder à votre contenu pendant la période à laquelle vous souhaitez autoriser l'accès.

   Si la demande répond aux exigences de la déclaration de politique, CloudFront effectue les opérations standard : détermine si le fichier se trouve déjà dans le cache périphérique, transmet la demande à l'origine si nécessaire et renvoie le fichier à l'utilisateur.

> **Note**
>
> Si une URL non signée contient des paramètres de chaîne de requête, assurez-vous de les inclure dans la partie de l'URL que vous signez. Si vous ajoutez une chaîne de requête à une URL signée après l'avoir signée, l'URL renvoie un code d'état HTTP 403.

> **Note**
>
> CloudFront ne nécessite pas d'URL signée ni de cookies signés pour les `OPTIONS` requêtes. Cela permet aux requêtes CORS Preflight, que les navigateurs envoient sans informations d'identification, de réussir pour les comportements de cache qui nécessitent des URL signées ou des cookies signés. Si les méthodes autorisées du comportement du cache incluent`OPTIONS`, CloudFront transmet les `OPTIONS` demandes à votre origine sans vérifier de signature. Assurez-vous que votre origine ne renvoie pas de contenu protégé en réponse à des `OPTIONS` demandes, ou limitez les méthodes autorisées à `GET` et `HEAD` si votre application n'utilise pas CORS.

Choix de la durée de validité des URL signées

Vous pouvez distribuer le contenu privé à l'aide d'une URL signée qui est valide pendant une brève durée, de quelques minutes au plus. Les URL signées qui sont valides pour une brève durée conviennent pour la distribution de contenu à la volée à un utilisateur à des fins spécifiques, telles que la distribution de locations de vidéos ou de téléchargements de musique aux clients à la demande. Si vos URL signées sont valides pour une brève période, vous voudrez probablement les générer automatiquement à l'aide d'une application que vous développez. Lorsque l'utilisateur commence à télécharger un fichier ou à lire un fichier multimédia, CloudFront compare le délai d'expiration de l'URL à l'heure actuelle pour déterminer si l'URL est toujours valide.

Vous pouvez aussi distribuer le contenu privé à l'aide d'une URL signée qui est valide pour une durée plus longue, quelques années peut-être. Les URL signées qui sont valides pendant une période plus longue sont utiles pour distribuer un contenu privé aux utilisateurs connus, comme la distribution d'un business plan aux investisseurs ou de documents de formation aux employés. Vous pouvez développer une application pour générer ces URL signées à plus long terme pour vous.

Quand CloudFront vérifie la date et l'heure d'expiration dans une URL signée

CloudFront vérifie la date et l'heure d'expiration dans une URL signée au moment de la requête HTTP. Si un client commence à télécharger un fichier volumineux immédiatement avant la date d'expiration, le téléchargement se termine même si la date d'expiration intervient pendant le téléchargement. Si la connexion TCP cesse et que le client essaie de redémarrer le téléchargement une fois la date d'expiration passée, le téléchargement échoue.

Si un client utilise des intervalles GET pour obtenir un fichier en parties plus petites, toute requête GET qui intervient après la date d'expiration échoue. Pour plus d'informations sur Range GET, consultez Comment CloudFront traite les demandes partielles pour un objet (range GETs).

Exemple de code et outils tiers

Pour obtenir un exemple de code qui crée la partie hachée et signée des URL signées, consultez les rubriques suivantes :

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework
- Créer une signature d'URL avec Java

Création d'une URL signée à l'aide d'une politique prédéfinie

Pour créer une URL signée à l'aide d'une politique prédéfinie, procédez comme suit.

Pour créer une URL signée à l'aide d'une politique prédéfinie

1. Si vous utilisez .NET ou Java pour créer des URL signées et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformatage de la clé privée (.NET et Java uniquement).
2. Concaténez les valeurs suivantes. Vous pouvez utiliser le format dans cet exemple d'URL signée.

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Expires=1767290400&Signature=nitfHRCrtziwO2HwPfWw~yYDhUF5Ew
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
```

```
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-Pair-Id=K2JCJMDEHXQW5F&Hash-Algorithm=SHA256
```

Supprimez tous les espaces vides (tabulations et sauts de ligne inclus). Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application. Toutes les valeurs ont le type `String`.

1. ***Base URL for the file***

   L'URL de base est l' CloudFront URL que vous utiliseriez pour accéder au fichier si vous n'utilisiez pas d'URL signées, y compris vos propres paramètres de chaîne de requête, le cas échéant. Dans l'exemple précédent, l'URL de base est `https://d111111abcdef8.cloudfront.net/image.jpg`. Pour plus d'informations sur le format des URL pour les distributions, consultez Personnalisez le format d'URL pour les fichiers dans CloudFront.

   - L' CloudFront URL suivante concerne un fichier image dans une distribution (utilisant le nom CloudFront de domaine). Notez que `image.jpg` se trouve dans un répertoire `images`. Le chemin d'accès au fichier de l'URL doit correspondre à celui du fichier de votre serveur HTTP ou de votre compartiment Amazon S3.

     ```
     https://d111111abcdef8.cloudfront.net/images/image.jpg
     ```

   - L' CloudFront URL suivante inclut une chaîne de requête :

     ```
     https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large
     ```

   - Les CloudFront URL suivantes concernent les fichiers image d'une distribution. Les deux utilisent un nom de domaine alternatif. La seconde inclut une chaîne de requête :

     ```
     https://www.example.com/images/image.jpg
     ```

     ```
     https://www.example.com/images/image.jpg?color=red
     ```

   - L' CloudFront URL suivante concerne un fichier image dans une distribution qui utilise un autre nom de domaine et le protocole HTTPS :

     ```
     https://www.example.com/images/image.jpg
     ```

2. **?**

   Le ? indique que les paramètres de requête suivent l'URL de base. Incluez le ? même si vous ne spécifiez aucun paramètre de requête.

> **Note**
>
> Vous pouvez spécifier les paramètres de requête suivants dans n'importe quel ordre.

3. ***Your query string parameters, if any*&**

   (Facultatif) Vous pouvez entrer vos propres paramètres de chaîne de requête. Pour ce faire, ajoutez une esperluette (&) entre chaque valeur, par exemple. `color=red&size=medium`. Vous pouvez spécifier les paramètres de chaîne de requête dans n'importe quel ordre dans l'URL.

   > **Important**
   >
   > Les paramètres de votre chaîne de requête ne peuvent pas être nommés `Expires`,`Signature`,`Key-Pair-Id`, ou`Hash-Algorithm`.

4. **Expires=*date and time in Unix time format (in seconds) and Coordinated Universal Time (UTC)***

   Date et heure auxquelles vous souhaitez que l'URL cesse d'autoriser l'accès au fichier.

   Spécifiez la date et l'heure d'expiration au format horaire Unix (en secondes) et en heure UTC. Par exemple, le 1er janvier 2026 à 10:00 UTC correspond à `1767290400` au format d'heure Unix, comme indiqué dans l'exemple au début de cette rubrique.

   Pour utiliser l'heure époque, indiquez un entier 64 bits correspondant à une date qui ne dépasse pas `9223372036854775807` (vendredi 11 avril 2262 à 23:47:16.854 UTC).

   Pour plus d'informations sur l'UTC, consultez RFC 3339, Date et heure sur Internet : Horodatages.

5. **&Signature=*hashed and signed version of the policy statement***

   Version hachée, signée et encodée en base 64 de la déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour une URL signée qui utilise une politique prédéfinie.

6. **&Key-Pair-Id=*public key ID for the CloudFront public key whose corresponding private key you're using to generate the signature***

   L'ID d'une clé CloudFront publique, par exemple,`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront quelle clé publique utiliser pour valider l'URL signée. CloudFront compare les informations de la signature à celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

   Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.

7. **&Hash-Algorithm=*SHA1 or SHA256***

   (Facultatif) Algorithme de hachage utilisé pour créer la signature. Les valeurs prises en charge sont `SHA1` et `SHA256`. Si vous ne spécifiez pas ce paramètre, sa CloudFront valeur par défaut est. `SHA1`

Création d'une signature pour une URL signée qui utilise une politique prédéfinie

Pour créer la signature pour une URL signée qui utilise une politique prédéfinie, suivez les procédures suivantes.

Rubriques

- Création d'une déclaration de politique pour une URL signée qui utilise une politique prédéfinie
- Création d'une signature pour une URL signée qui utilise une politique prédéfinie

Création d'une déclaration de politique pour une URL signée qui utilise une politique prédéfinie

Lorsque vous créez une URL signée avec une politique prédéfinie, le paramètre `Signature` est une version hachée et signée d'une déclaration de politique. Pour les URL signées qui utilisent une politique prédéfinie, vous n'incluez pas la déclaration de politique dans l'URL, comme vous le faites pour les URL signées qui utilisent une politique personnalisée. Pour créer la déclaration de politique, effectuez la procédure suivante.

Pour créer la déclaration de politique d'une URL signée qui utilise une politique prédéfinie

1. Construisez la déclaration de politique en utilisant le format JSON suivant et en utilisant UTF-8 le codage de caractères. Incluez la ponctuation et les autres valeurs littérales exactement comme

spécifié. Pour plus d'informations sur les paramètres `Resource` et `DateLessThan`, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique prédéfinie.

```
{
    "Statement": [
        {
            "Resource": "base URL or stream name",
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": ending date and time in Unix time format and
 UTC
                }
            }
        }
    ]
}
```

2. Supprimez tous les espaces vides (tabulations et sauts de ligne inclus) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.

Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique prédéfinie

Lorsque vous créez une déclaration de politique pour une politique prédéfinie, vous spécifiez les valeurs suivantes.

Ressource

> **Note**
>
> Vous ne pouvez spécifier qu'une seule valeur pour `Resource`.

L'URL de base, y compris les chaînes de votre requête, le cas échéant CloudFront `Expires`, mais en excluant `Hash-Algorithm` les paramètres `SignatureKey-Pair-Id`,, et, par exemple :

`https://d111111abcdef8.cloudfront.net/images/horizon.jpg?size=large&license=yes`

Notez ce qui suit :

- Protocole : la valeur doit commencer par `http://` ou `https://`.
- Paramètres de chaîne de requête : si vous n'avez aucun paramètre de chaîne de requête, omettez le point d'interrogation.
- Noms de domaine alternatifs : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL, vous devez le spécifier lorsque vous référencez le fichier dans votre page ou application web. Ne spécifiez pas l'URL Amazon S3 pour l'objet.
- Caractères spéciaux : si l'URL de votre ressource contient un astérisque (*) ou un point d'interrogation (?) (par exemple, dans le nom de la clé de l'objet), vous devez utiliser URL-encode ces caractères (`%2A`pour * et `%3F` pour?). Cela est dû au fait qu'il CloudFront interprète les caractères non codés * et comme ? des caractères génériques dans le chemin de la ressource. Si ces caractères ne le sont pas URL-encoded, l'URL signée peut accorder un accès plus large que prévu.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. Par exemple, le 1er janvier 2026 à 10 h UTC est converti en 1767290400 au format d'heure Unix.

Cette valeur doit correspondre à la valeur du paramètre de la chaîne de requête `Expires` de l'URL signée. N'entourez pas la valeur de points d'interrogation.

Pour plus d'informations, consultez Quand CloudFront vérifie la date et l'heure d'expiration dans une URL signée.

Exemple d'une déclaration de politique pour une URL signée qui utilise une politique prédéfinie

Lorsque vous utilisez l'exemple de déclaration de politique suivant dans une URL signée, un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/horizon.jpg` jusqu'au 1er janvier 2026 à 10 h UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
```

```
            "Condition": {
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Création d'une signature pour une URL signée qui utilise une politique prédéfinie

Pour créer la valeur du paramètre `Signature` d'une URL signée, vous hachez et signez la déclaration de politique que vous avez créée dans Création d'une déclaration de politique pour une URL signée qui utilise une politique prédéfinie.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez :

- Utilisation d'une commande Linux et OpenSSL pour le chiffrement et l'encodage en base64
- Exemples de code pour la création de la signature d'une URL signée

> **Note**
>
> Les exemples liés sont utilisés SHA-1 par défaut. Pour l'utiliser à la SHA-256 place, remplacez `sha1` par `sha256` dans les commandes OpenSSL et incluez le paramètre de `Hash-Algorithm=SHA256` requête dans l'URL signée.

Option 1 : Créer une signature à l'aide d'une politique prédéfinie

1. Utilisez la fonction de SHA-256 hachage SHA-1 or et la clé privée RSA ou ECDSA générée pour hacher et signer la déclaration de politique que vous avez créée dans la procédure. Pour créer la déclaration de politique d'une URL signée qui utilise une politique prédéfinie Utilisez la version de la déclaration de politique qui n'inclut plus d'espaces vides.

   Si vous utilisez SHA-256, vous devez inclure `&Hash-Algorithm=SHA256` dans l'URL signée.

   Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

> **Note**
>
> La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (tabulations et sauts de ligne inclus) de la chaîne hachée et signée.
3. Base64-encode la chaîne utilisant le codage MIME base64. Pour plus d'informations, consultez la Section 6.8, Base64 Content-Transfer-Encoding de la RFC 2045, MIME (Multipurpose Internet Mail Extensions), première partie : Format des corps des messages Internet.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Ajoutez la valeur obtenue à votre URL signée après `&Signature=`, et retournez à Pour créer une URL signée à l'aide d'une politique prédéfinie pour terminer la concaténation des parties de votre URL signée.

Création d'une URL signée utilisant une politique personnalisée

Pour créer une URL signée utilisant une politique personnalisée, suivez la procédure suivante.

Pour créer une URL signée utilisant une politique personnalisée

1. Si vous utilisez .NET ou Java pour créer des URL signées et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformatage de la clé privée (.NET et Java uniquement).
2. Concaténez les valeurs suivantes. Vous pouvez utiliser le format dans cet exemple d'URL signée.

```
https://d111111abcdef8.cloudfront.net/
image.jpg?color=red&size=medium&Policy=eyANCiAgICEXAMPLEW1lbnQiOiBbeyANCiAgICAgICJSZXNvdXJj
j19DzZrvDh6hQ73lDx~-ar3UocvvRQVw6EkC~GdpGQyyOSKQim-
TxAnW7d8F5Kkai9HVx0FIu-5jcQb0UEmatEXAMPLE3ReXySpLSMj0yCd3ZAB4UcBCAqEijkytL6f3fVYNGQI6&Key-
Pair-Id=K2JCJMDEHXQW5F&Hash-Algorithm=SHA256
```

Supprimez tous les espaces vides (tabulations et sauts de ligne inclus). Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application. Toutes les valeurs ont le type `String`.

1. ***Base URL for the file***

   L'URL de base est l' CloudFront URL que vous utiliseriez pour accéder au fichier si vous n'utilisiez pas d'URL signées, y compris vos propres paramètres de chaîne de requête, le cas échéant. Dans l'exemple précédent, l'URL de base est `https://d111111abcdef8.cloudfront.net/image.jpg`. Pour plus d'informations sur le format des URL pour les distributions, consultez Personnalisez le format d'URL pour les fichiers dans CloudFront.

   Les exemples suivants affichent les valeurs que vous spécifiez pour les distributions.

   - L' CloudFront URL suivante concerne un fichier image dans une distribution (utilisant le nom CloudFront de domaine). Notez que `image.jpg` se trouve dans un répertoire `images`. Le chemin d'accès au fichier de l'URL doit correspondre à celui du fichier de votre serveur HTTP ou de votre compartiment Amazon S3.

     ```
     https://d111111abcdef8.cloudfront.net/images/image.jpg
     ```

   - L' CloudFront URL suivante inclut une chaîne de requête :

     ```
     https://d111111abcdef8.cloudfront.net/images/image.jpg?size=large
     ```

   - Les CloudFront URL suivantes concernent les fichiers image d'une distribution. Les deux utilisent un nom de domaine alternatif ; le second inclut une chaîne de requête :

     ```
     https://www.example.com/images/image.jpg
     ```

     ```
     https://www.example.com/images/image.jpg?color=red
     ```

   - L' CloudFront URL suivante concerne un fichier image dans une distribution qui utilise un autre nom de domaine et le protocole HTTPS :

```
https://www.example.com/images/image.jpg
```

2. **?**

   Le ? indique que les paramètres de chaîne de requête suivent l'URL de base. Incluez le ? même si vous ne spécifiez aucun paramètre de requête.

   > **Note**
   >
   > Vous pouvez spécifier les paramètres de requête suivants dans n'importe quel ordre.

3. ***Your query string parameters, if any*&**

   (Facultatif) Vous pouvez entrer vos propres paramètres de chaîne de requête. Pour ce faire, ajoutez une esperluette (&) entre chaque valeur, par exemple. `color=red&size=medium`. Vous pouvez spécifier les paramètres de chaîne de requête dans n'importe quel ordre dans l'URL.

   > **Important**
   >
   > Les paramètres de votre chaîne de requête ne peuvent pas être nommés `PolicySignature`,`Key-Pair-Id`, ou`Hash-Algorithm`.

   Si vous ajoutez vos propres paramètres, ajoutez un & après chacun d'eux, y compris le dernier.

4. **Policy=*base64 encoded version of policy statement***

   Votre déclaration de politique au format JSON, avec suppression des espaces vide, puis encodage en base64. Pour plus d'informations, consultez Création d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée.

   La déclaration de politique contrôle l'accès accordé par une URL signée à un utilisateur. Elle inclut l'URL du fichier, une date et une heure d'expiration, une date et une heure (facultatif) auxquelles l'URL devient valide et une adresse IP (facultatif) ou une plage d'adresses IP autorisées à accéder au fichier.

5. **&Signature=*hashed and signed version of the policy statement***

   Version hachée, signée et encodée en base 64 de la déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour une URL signée qui utilise une politique personnalisée.

6. **&Key-Pair-Id=*public key ID for the CloudFront public key whose corresponding private key you're using to generate the signature***

   L'ID d'une clé CloudFront publique, par exemple`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront quelle clé publique utiliser pour valider l'URL signée. CloudFrontcompare les informations de la signature à celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

   Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.

7. **&Hash-Algorithm=*SHA1 or SHA256***

   (Facultatif) Algorithme de hachage utilisé pour créer la signature. Les valeurs prises en charge sont `SHA1` et `SHA256`. Si vous ne spécifiez pas ce paramètre, sa CloudFront valeur par défaut est. `SHA1`

Création d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée

Effectuez la procédure suivante pour créer une déclaration de politique pour une URL signée qui utilise une politique personnalisée.

Pour obtenir des exemples de déclaration de politique qui contrôlent l'accès aux fichiers de différentes façons, consultez the section called "Exemple d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée".

Pour créer la déclaration de politique d'une URL signée qui utilise une politique personnalisée

1. Construisez la déclaration de politique à l'aide du format JSON suivant. Remplacez les symboles inférieur à (<) et supérieur à (>), ainsi que les descriptions qu'ils contiennent, par vos propres valeurs. Pour plus d'informations, consultez the section called "Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée".

   ```
   {
   ```

```
    "Statement": [
        {
            "Resource": "<Optional but recommended: URL of the file>",
            "Condition": {
                "DateLessThan": {
                 "AWS:EpochTime": <Required: ending date and time in Unix time
 format and UTC>
                },
                "DateGreaterThan": {
                 "AWS:EpochTime": <Optional: beginning date and time in Unix time
 format and UTC>
                },
                "IpAddress": {
                 "AWS:SourceIp": "<Optional: IP address>"
                }
            }
        }
    ]
}
```

Notez ce qui suit :

- Vous pouvez inclure une seule déclaration dans cette politique.
- Utilisez UTF-8 le codage des caractères.
- Incluez la ponctuation et les noms de paramètre exactement comme spécifié. Les abréviations ne sont pas acceptées pour les noms de paramètre.
- L'ordre des paramètres de la section `Condition` n'importe pas.
- Pour plus d'informations sur les valeurs de `Resource`, `DateLessThan`, `DateGreaterThan` et `IpAddress`, consultez the section called "Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée".

2. Supprimez tous les espaces vides (tabulations et sauts de ligne inclus) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.
3. Base64-encode la déclaration de politique utilisant le codage MIME base64. Pour plus d'informations, consultez la Section 6.8, Base64 Content-Transfer-Encoding de la RFC 2045, MIME (Multipurpose Internet Mail Extensions), première partie : Format des corps des messages Internet.

4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Ajoutez la valeur obtenue à votre URL signée après `Policy=`.
6. Créez une signature pour l'URL signée en hachant, signant et encodant en base64 la déclaration de politique. Pour plus d'informations, consultez the section called "Création d'une signature pour une URL signée qui utilise une politique personnalisée".

Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée

Lorsque vous créez une déclaration de politique pour une politique personnalisée, vous spécifiez les valeurs suivantes.

Ressource

URL, y compris toutes les chaînes de requête, mais à l'exclusion des `Hash-Algorithm` paramètres CloudFront `Policy` `SignatureKey-Pair-Id`,, et. Par exemple :

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg\?
size=large&license=yes
```

Vous ne pouvez spécifier qu'une seule valeur d'URL pour `Resource`.

> **Important**
>
> Vous pouvez omettre le paramètre `Resource` dans une politique, mais cela signifie que toute personne disposant de l'URL signée peut accéder à tous les fichiers de toute distribution associée à cette paire de clés que vous utilisez pour créer l'URL signée.

Notez ce qui suit :

- Protocole : la valeur doit commencer par `http://`, `https://` ou `*://`.
- Paramètres de chaîne de requête : si l'URL contient des paramètres de chaîne de requête, n'utilisez pas de barre oblique inverse (\) pour échapper au point d'interrogation (?) qui commence la chaîne de requête. Par exemple :

  ```
  https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
  size=large&license=yes
  ```

- Caractères génériques : vous pouvez utiliser des caractères génériques dans l'URL de la politique. Les caractères génériques suivants sont pris en charge :
  - astérisque (*), qui correspond à zéro, un ou plusieurs caractères
  - point d'interrogation (?), qui correspond à un et un seul caractère

  Lorsque l'URL de la politique CloudFront correspond à l'URL de la requête HTTP, l'URL de la stratégie est divisée en quatre sections (protocole, domaine, chemin et chaîne de requête) comme suit :

  ```
  [protocol]://[domain]/[path]\?[query string]
  ```

  Lorsque vous utilisez un caractère générique dans l'URL de la politique, la correspondance avec le caractère générique s'applique uniquement dans les limites de la section qui contient ce caractère générique. Par exemple, envisagez l'URL suivante dans une politique :

  ```
  https://www.example.com/hello*world
  ```

  Dans cet exemple, le caractère générique astérisque (*) s'applique uniquement dans la section du chemin. Il correspond donc aux URL `https://www.example.com/helloworld` et `https://www.example.com/hello-world`, mais il ne correspond pas à l'URL `https://www.example.net/hello?world`.

  Les exceptions suivantes s'appliquent aux limites des sections pour la mise en correspondance des caractères génériques :

  - La présence d'un astérisque à la fin de la section de chemin implique un astérisque dans la section de la chaîne de requête. Par exemple, `http://example.com/hello*` équivaut à `http://example.com/hello*\?*`.
  - La présence d'un astérisque à la fin de la section de domaine implique un astérisque dans les sections de chemin et de chaîne de requête. Par exemple, `http://example.com*` équivaut à `http://example.com*/*\?*`.

- Une URL figurant dans la politique peut omettre la section de protocole et commencer par un astérisque dans la section de domaine. Dans ce cas, la section de protocole est implicitement définie sur un astérisque. Par exemple, l'URL `*example.com` d'une politique est équivalente à `*://*example.com/`.
- Un astérisque à lui seul (`"Resource": "*"`) correspond à n'importe quelle URL.

Par exemple, la valeur `https://d111111abcdef8.cloudfront.net/*game_download.zip*` dans une politique correspond à toutes les URL suivantes :

- `https://d111111abcdef8.cloudfront.net/game_download.zip`
- `https://d111111abcdef8.cloudfront.net/example_game_download.zip?license=yes`
- `https://d111111abcdef8.cloudfront.net/test_game_download.zip?license=temp`

Percent-encoded caractères : fait CloudFront correspondre la politique `Resource` à l'URL de demande brute (non décodée) et transmet cette URL à l'origine sans modification. Un caractère codé en pourcentage dans l'URL de la demande, tel que `%3B` for `;`, for ou `%3F` `%23` for `?#`, est traité comme des données plutôt que comme un délimiteur d'URL. Pour plus d'informations, consultez la RFC 3986 sur le site web de l'IETF. Par exemple, un caractère générique ne peut pas correspondre à un point-virgule littéral (`;`), mais il peut correspondre à la forme codée (). `%3B`

- Autres noms de domaine : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL de la politique, la requête HTTP doit utiliser ce nom de domaine alternatif dans votre page ou application Web. Ne spécifiez pas l'URL Amazon S3 pour le fichier dans une politique.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. Dans la politique, n'entourez pas la valeur avec des points d'interrogation. Pour plus d'informations sur l'UTC, consultez Date et heure sur Internet : Horodatages.

Par exemple, l'horodatage 31 janvier 2023 10 h 00 UTC est converti en 1675159200 au format horaire Unix.

Il s'agit du seul paramètre obligatoire de `Condition` cette section. CloudFront requiert cette valeur pour empêcher les utilisateurs d'avoir un accès permanent à votre contenu privé.

Pour plus d'informations, consultez the section called "Quand CloudFront vérifie la date et l'heure d'expiration dans une URL signée"

DateGreaterThan (Facultatif)

(Facultatif) Date et heure de début de l'URL au format horaire Unix (en secondes) et en heure UTC. Les utilisateurs ne sont pas autorisés à accéder au fichier avant la date et l'heure spécifiées. N'entourez pas la valeur de points d'interrogation.

IpAddress (Facultatif)

Adresse IP du client formulant la requête HTTP. Notez ce qui suit :

- Pour autoriser une adresse IP à accéder au fichier, omettez le paramètre `IpAddress`.
- Vous pouvez spécifier une adresse IP ou une plage d'adresses IP. Vous ne pouvez pas utiliser cette politique pour autoriser l'accès si l'adresse IP du client figure dans l'une des deux plages distinctes.
- Pour autoriser l'accès depuis une seule adresse IP, vous spécifiez :

  `"IPv4 IP address/32"`
- Vous devez spécifier les plages d'adresses IP selon le format IPv4 CIDR standard (par exemple, `192.0.2.0/24`). Pour plus d'informations, voir Inter-domain Routage sans classe (CIDR) : le plan d'attribution et d'agrégation d'adresses Internet.

> **Important**
>
> Les adresses IP au format IPv6, telles que 2001:0db8:85a3::8a2e:0370:7334, ne sont pas prises en charge.

Si vous utilisez une politique personnalisée qui inclut `IpAddress`, n'activez pas IPv6 pour la distribution. Si vous souhaitez limiter l'accès à un contenu spécifique par adresse IP et prendre en charge les requêtes IPv6 pour les autres contenus, vous pouvez créer deux distributions. Pour plus d'informations, consultez the section called "Activation d'IPv6 (demandes des utilisateurs)" dans la rubrique the section called "Tous les paramètres de distribution".

Exemple d'une déclaration de politique pour une URL signée qui utilise une politique personnalisée

Les exemples suivants de déclaration de politique montrent comment accéder à un fichier spécifique, à tous les objets d'un répertoire ou à tous les fichiers associés à un ID de paire de clés. Les

exemples montrent aussi comment contrôler l'accès depuis une adresse IP individuelle ou une plage d'adresses IP, et comment empêcher les utilisateurs d'employer l'URL signée au-delà d'une date et heure spécifiées.

Si vous copiez et collez l'un de ces exemples, supprimez les espaces vides (y compris les tabulations et les sauts de ligne), remplacez les valeurs par vos propres valeurs et incluez un caractère de saut de ligne après l'accolade fermante (}).

Pour plus d'informations, consultez the section called "Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée".

Rubriques

- Exemple de déclaration de politique : accès à un fichier à partir d'une plage d'adresses IP
- Exemple de déclaration de politique : accès à tous les fichiers d'un répertoire à partir d'une plage d'adresses IP
- Exemple de déclaration de politique : accès à tous les fichiers associés à un ID de paire de clés à partir d'une adresse IP

Exemple de déclaration de politique : accès à un fichier à partir d'une plage d'adresses IP

L'exemple suivant de politique personnalisée dans une URL signée spécifie qu'un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/game_download.zip` à partir des adresses IP de la plage `192.0.2.0/24` jusqu'au 31 janvier 2023 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/game_download.zip",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675159200
                }
            }
        }
    ]
}
```

Exemple de déclaration de politique : accès à tous les fichiers d'un répertoire à partir d'une plage d'adresses IP

À l'aide de l'exemple de politique personnalisée suivant, vous pouvez créer des URL signées pour n'importe quel fichier du `training` répertoire, comme indiqué par le caractère générique astérisque (*) dans le `Resource` paramètre. Les utilisateurs peuvent accéder au fichier depuis une adresse IP de la plage `192.0.2.0/24` jusqu'au 31 janvier 2023 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675159200
                }
            }
        }
    ]
}
```

Chaque URL signée avec laquelle vous utilisez cette politique inclut une URL qui identifie un fichier spécifique ; par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Exemple de déclaration de politique : accès à tous les fichiers associés à un ID de paire de clés à partir d'une adresse IP

À l'aide de l'exemple de politique personnalisée suivant, vous pouvez créer des URL signées pour n'importe quel fichier associé à une distribution, comme indiqué par le caractère générique astérisque (*) dans le `Resource` paramètre. L'URL signée doit utiliser le protocole `https://`, et non `http://`. L'utilisateur doit employer l'adresse IP `192.0.2.10/32`. (La valeur `192.0.2.10/32` en notation CIDR fait référence à une seule adresse IP, `192.0.2.10`.) Les fichiers ne sont disponibles qu'entre le 31 janvier 2023 10 h 00 UTC et le 2 février 2023 10 h 00 UTC :

```
{
```

```
    "Statement": [
       {
            "Resource": "https://*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1675159200
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1675332000
                }
            }
         }
    ]
}
```

Chaque URL signée avec laquelle vous utilisez cette politique possède une URL qui identifie un fichier spécifique dans une CloudFront distribution spécifique, par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

L'URL signée inclut aussi un ID de paire de clés, qui doit être associé à un groupe de clés autorisé dans la distribution (d111111abcdef8.cloudfront.net) que vous spécifiez dans l'URL.

Création d'une signature pour une URL signée qui utilise une politique personnalisée

La signature d'une URL signée utilisant une politique personnalisée est une version hachée, signée et encodée en base64 de la déclaration de politique. Pour créer une signature pour une politique personnalisée, procédez comme suit.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez :

- Utilisation d'une commande Linux et OpenSSL pour le chiffrement et l'encodage en base64
- Exemples de code pour la création de la signature d'une URL signée

> **Note**
>
> Les exemples liés sont utilisés SHA-1 par défaut. Pour l'utiliser à la SHA-256 place, remplacez `sha1` par `sha256` dans les commandes OpenSSL et incluez le paramètre de `Hash-Algorithm=SHA256` requête dans l'URL signée.

Option 1 : Créer une signature à l'aide d'une politique personnalisée

1. Utilisez la fonction de SHA-256 hachage SHA-1 or et la clé privée RSA ou ECDSA générée pour hacher et signer la déclaration de politique JSON que vous avez créée au cours de la procédure. Pour créer la déclaration de politique d'une URL signée qui utilise une politique personnalisée Utilisez la version de la déclaration de politique qui n'inclut plus d'espaces vides, mais qui n'a pas encore été encodée en base64.

   Si vous utilisez SHA-256, vous devez inclure `&Hash-Algorithm=SHA256` dans l'URL signée.

   Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

   > **Note**
   >
   > La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (tabulations et sauts de ligne inclus) de la chaîne hachée et signée.
3. Base64-encode la chaîne utilisant le codage MIME base64. Pour plus d'informations, consultez la Section 6.8, Base64 Content-Transfer-Encoding de la RFC 2045, MIME (Multipurpose Internet Mail Extensions), première partie : Format des corps des messages Internet.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)

Remplacer ces caractères non valides	Par ces caractères valides
=	_ (soulignement)
/	~ (tilde)

5. Ajoutez la valeur obtenue à votre URL signée après `&Signature=`, et retournez à Pour créer une URL signée utilisant une politique personnalisée pour terminer la concaténation des parties de votre URL signée.

Utilisation de cookies signés

CloudFront les cookies signés vous permettent de contrôler qui peut accéder à votre contenu lorsque vous ne souhaitez pas modifier vos URL actuelles ou lorsque vous souhaitez donner accès à plusieurs fichiers restreints, par exemple tous les fichiers de la zone réservée aux abonnés d'un site Web. Cette rubrique explique l'utilisation des cookies signés et décrit comment les définir à l'aide de politiques prédéfinies et personnalisées.

Rubriques

- Choix entre des politiques prédéfinies et personnalisées pour les cookies signés
- Fonctionnement des cookies signés
- Prévention du mauvais usage des cookies signés
- Quand CloudFront vérifie la date et l'heure d'expiration d'un cookie signé
- Exemple de code et outils tiers
- Définition de cookies signés à l'aide d'une politique prédéfinie
- Définition de cookies signés utilisant une politique personnalisée
- Création de cookies signés avec PHP

Choix entre des politiques prédéfinies et personnalisées pour les cookies signés

Lorsque vous créez un cookie signé, vous écrivez une instruction de politique au format JSON qui spécifie les restrictions sur le cookie signé : par exemple, la durée de validité du cookie. Vous pouvez utiliser une politique prédéfinie ou une politique personnalisé e. Le tableau suivant compare les politiques prédéfinies et les politiques personnalisées :

Description	Politique prédéfinie	Politique personnalisée
Vous pouvez réutiliser la déclaration de politique pour plusieurs fichiers. Pour ce faire, vous devez utiliser les caractères génériques de l'objet `Resource`. Pour plus d'informations, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés.)	Non	Oui
Vous pouvez indiquer la date et l'heure auxquelles les utilisateurs peuvent commencer à accéder à votre contenu	Non	Oui (facultatif)
Vous pouvez indiquer la date et l'heure auxquelles les utilisateurs ne peuvent plus accéder à votre contenu	Oui	Oui
Vous pouvez spécifier l'adresse IP ou la plage d'adresses IP des utilisateurs qui peuvent accéder à votre contenu	Non	Oui (facultatif)

Pour plus d'informations sur la création de cookies signés à l'aide d'une politique prédéfinie, consultez Définition de cookies signés à l'aide d'une politique prédéfinie.

Pour plus d'informations sur la création de cookies signés à l'aide d'une politique personnalisée, consultez Définition de cookies signés utilisant une politique personnalisée.

Fonctionnement des cookies signés

Voici un aperçu de la façon dont vous configurez CloudFront les cookies signés et de la façon dont vous CloudFront répondez lorsqu'un utilisateur soumet une demande contenant un cookie signé.

1. Dans votre CloudFront distribution, spécifiez un ou plusieurs groupes de clés fiables, qui contiennent les clés publiques que CloudFront vous pouvez utiliser pour vérifier la signature de l'URL. Vous utilisez les clés privées correspondantes pour signer les URL.

Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.

2. Vous développez votre application pour déterminer si un utilisateur doit avoir accès à votre contenu et, si tel est le cas, pour envoyer trois en-têtes `Set-Cookie` à l'utilisateur. (Chaque `Set-Cookie` en-tête ne peut contenir qu'une seule paire nom-valeur, et un cookie CloudFront signé nécessite trois paires nom-valeur.) Vous devez envoyer les en-têtes `Set-Cookie` à l'utilisateur avant qu'il ne demande votre contenu privé. Si vous définissez une durée d'expiration brève sur le cookie, il se peut aussi que vous vouliez envoyer trois en-têtes `Set-Cookie` supplémentaires en réponse aux demandes suivantes, de telle sorte que l'utilisateur puisse continuer à y accéder.

   En règle générale, votre CloudFront distribution aura au moins deux comportements de cache, l'un ne nécessitant pas d'authentification et l'autre nécessitant une authentification. La page d'erreur de la partie sécurisé du site inclut une redirection ou un lien vers une page de connexion.

   Si vous configurez votre distribution pour mettre en cache des fichiers basés sur des cookies, CloudFront elle ne met pas en cache des fichiers distincts en fonction des attributs des cookies signés.
3. Un utilisateur se connecte à votre site web et paie le contenu ou satisfait à quelques autres exigences pour l'accès.
4. Votre application renvoie les en-têtes `Set-Cookie` dans la réponse, et l'utilisateur stocke les paires nom-valeur.
5. L'utilisateur demande un fichier.

   Le navigateur de cet utilisateur ou d'un autre obtient les paires nom-valeur de l'étape 4 et les ajoute à la demande dans un en-tête `Cookie`. Il s'agit du cookie signé.
6. CloudFront utilise la clé publique pour valider la signature dans le cookie signé et pour confirmer que le cookie n'a pas été falsifié. Si la signature n'est pas valide, la demande est rejetée.

   Si la signature du cookie est valide, CloudFront examine la déclaration de politique contenue dans le cookie (ou en crée une si vous utilisez une politique prédéfinie) pour confirmer que la demande est toujours valide. Par exemple, si vous avez spécifié une date et une heure de début et de fin pour le cookie, cela CloudFront confirme que l'utilisateur essaie d'accéder à votre contenu pendant la période à laquelle vous souhaitez autoriser l'accès.

Si la demande répond aux exigences de la déclaration de politique, CloudFront diffuse votre contenu de la même manière que pour le contenu non restreint : elle détermine si le fichier se trouve déjà dans le cache périphérique, transmet la demande à l'origine si nécessaire et renvoie le fichier à l'utilisateur.

> **Note**
>
> CloudFront ne nécessite pas d'URL signée ni de cookies signés pour les `OPTIONS` requêtes. Cela permet aux requêtes CORS Preflight, que les navigateurs envoient sans informations d'identification, de réussir pour les comportements de cache qui nécessitent des URL signées ou des cookies signés. Si les méthodes autorisées du comportement du cache incluent`OPTIONS`, CloudFront transmet les `OPTIONS` demandes à votre origine sans vérifier de signature. Assurez-vous que votre origine ne renvoie pas de contenu protégé en réponse à des `OPTIONS` demandes, ou limitez les méthodes autorisées à `GET` et `HEAD` si votre application n'utilise pas CORS.

Prévention du mauvais usage des cookies signés

Si vous spécifiez le paramètre `Domain` dans un en-tête `Set-Cookie`, spécifiez la valeur la plus précise possible pour réduire les possibilités d'accès par une personne ayant le même nom de domaine racine. Par exemple, app.example.com est préférable à example.com, particulièrement quand vous ne contrôlez pas example.com. Vous empêchez ainsi qu'une personne accède à votre contenu depuis www.example.com.

Pour contribuer à empêcher ce type d'attaque, procédez comme suit :

- Excluez les attributs de cookie `Expires` et `Max-Age`, de telle sorte que l'en-tête `Set-Cookie` crée un cookie de session. Les cookies de session sont automatiquement supprimés quand l'utilisateur clôt le navigateur, ce qui réduit la possibilité que quelqu'un n'obtienne un accès non autorisé à votre contenu.
- Incluez l'attribut `Secure`, de telle sorte que le cookie soit chiffré quand un utilisateur l'inclut dans une demande.
- Chaque fois que possible, utilisez une politique personnalisée et incluez l'adresse IP de l'utilisateur.
- Dans l'attribut `CloudFront-Expires`, spécifiez la durée d'expiration raisonnable la plus courte selon la période pendant laquelle vous autorisez les utilisateurs à accéder à votre contenu.

Quand CloudFront vérifie la date et l'heure d'expiration d'un cookie signé

Pour déterminer si un cookie signé est toujours valide, CloudFront vérifie la date et l'heure d'expiration du cookie au moment de la requête HTTP. Si un client commence à télécharger un fichier volumineux immédiatement avant la date d'expiration, le téléchargement se termine même si la date d'expiration intervient pendant le téléchargement. Si la connexion TCP cesse et que le client essaie de redémarrer le téléchargement une fois la date d'expiration passée, le téléchargement échoue.

Si un client utilise des intervalles GET pour obtenir un fichier en parties plus petites, toute requête GET qui intervient après la date d'expiration échoue. Pour plus d'informations sur Range GET, consultez Comment CloudFront traite les demandes partielles pour un objet (range GETs).

Exemple de code et outils tiers

L'exemple de code de contenu privé montre uniquement comment créer la signature pour les URL signées. Cependant, le processus de création d'une signature d'un cookie signé étant très similaire, une grande partie de l'exemple de code continue à être pertinente. Pour plus d'informations, consultez les rubriques suivantes :

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework
- Créer une signature d'URL avec Java

Définition de cookies signés à l'aide d'une politique prédéfinie

Pour définir un cookie signé à l'aide d'une politique prédéfinie, procédez comme suit. Pour créer la signature, consultez Création d'une signature pour un cookie signé qui utilise une politique prédéfinie.

Pour définir un cookie signé à l'aide d'une politique prédéfinie

1. Si vous utilisez .NET ou Java pour créer des cookies signés et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformatage de la clé privée (.NET et Java uniquement).
2. Programmez votre application pour envoyer trois `Set-Cookie` en-têtes aux spectateurs approuvés (ou quatre, si vous souhaitez spécifier un algorithme de hachage). Vous avez besoin de trois en-têtes `Set-Cookie` parce que chaque en-tête `Set-Cookie` ne peut contenir

qu'une seule paire nom-valeur, et qu'un cookie signé CloudFront nécessite trois paires nom-valeur. Les paires nom-valeur sont : `CloudFront-Expires`, `CloudFront-Signature` et `CloudFront-Key-Pair-Id`. Vous pouvez éventuellement inclure une quatrième paire nom-valeur,`CloudFront-Hash-Algorithm`, pour spécifier l'algorithme de hachage utilisé pour la signature. Les valeurs doivent être présentes sur la visionneuse avant qu'un utilisateur ne puisse faire la requête d'un fichier dont vous voulez contrôler l'accès.

> **Note**
>
> En règle générale, nous recommandons d'exclure les attributs `Expires` et `Max-Age`. L'exclusion des attributs conduit le navigateur à supprimer le cookie quand l'utilisateur ferme le navigateur, ce qui réduit la possibilité qu'une personne obtienne un accès non autorisé à votre contenu. Pour plus d'informations, consultez Prévention du mauvais usage des cookies signés.

Les noms des attributs de cookie sont sensibles à la casse.

Les sauts de ligne ne sont inclus que pour rendre les attributs plus lisibles.

```
Set-Cookie:
CloudFront-Expires=date and time in Unix time format (in seconds) and Coordinated
 Universal Time (UTC);
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly

Set-Cookie:
CloudFront-Signature=hashed and signed version of the policy statement;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly

Set-Cookie:
CloudFront-Key-Pair-Id=public key ID for the CloudFront public key whose
 corresponding private key you're using to generate the signature;
Domain=optional domain name;
Path=/optional directory path;
Secure;
```

```
HttpOnly

Set-Cookie:
CloudFront-Hash-Algorithm=SHA1 or SHA256;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly
```

(Facultatif) **`Domain`**

Nom de domaine du fichier demandé. Si vous ne spécifiez pas un attribut `Domain`, la valeur par défaut est le nom de domaine de l'URL et ne s'applique qu'au nom de domaine spécifié, non aux sous-domaines. Si vous spécifiez un attribut `Domain`, il s'applique aussi aux sous-domaines. Un point devant le nom de domaine (par exemple, `Domain=.example.com`) est facultatif. De plus, si vous spécifiez un attribut `Domain`, le nom de domaine de l'URL et la valeur de l'attribut `Domain` doivent correspondre.

Vous pouvez spécifier le nom de domaine CloudFront attribué à votre distribution, par exemple, d111111abcdef8.cloudfront.net, mais vous ne pouvez pas spécifier *.cloudfront.net pour le nom de domaine.

Si vous souhaitez utiliser un nom de domaine alternatif tel qu'example.com dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez l'attribut `Domain` ou non. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence de tous les paramètres de distribution.

(Facultatif) **`Path`**

Chemin d'accès du fichier demandé. Si vous ne spécifiez pas d'attribut `Path`, la valeur par défaut est le chemin d'accès de l'URL.

`Secure`

Nécessite que l'utilisateur chiffre les cookies avant d'envoyer une demande. Nous vous recommandons d'envoyer l'`Set-Cookie`en-tête via une connexion HTTPS pour vous assurer que les attributs des cookies sont protégés contre les attaques de type man-in-the-middle.

`HttpOnly`

Définit la manière dont le navigateur (lorsqu'il est pris en charge) interagit avec la valeur du cookie. Avec`HttpOnly`, les valeurs des cookies sont inaccessibles à JavaScript.

Cette précaution permet d'atténuer les attaques par scripts inter-site (XSS). Pour plus d'informations, consultez Utilisation de cookies HTTPS.

`CloudFront-Expires`

Spécifiez la date et l'heure d'expiration au format horaire Unix (en secondes) et en heure UTC. Par exemple, le 1er janvier 2026 à 10 h UTC est converti en 1767290400 au format d'heure Unix.

Pour utiliser l'heure époque, indiquez un entier 64 bits correspondant à une date qui ne dépasse pas `9223372036854775807` (vendredi 11 avril 2262 à 23:47:16.854 UTC).

Pour plus d'informations sur l'UTC, consultez RFC 3339, Date et heure sur Internet : Horodatages, https://tools.ietf.org/html/rfc3339.

`CloudFront-Signature`

Version hachée, signée et encodée en base 64 d'une déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique prédéfinie.

`CloudFront-Key-Pair-Id`

L'ID d'une clé CloudFront publique, par exemple`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront quelle clé publique utiliser pour valider l'URL signée. CloudFront compare les informations de la signature à celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.

`CloudFront-Hash-Algorithm`

(Facultatif) Algorithme de hachage utilisé pour créer la signature. Les valeurs prises en charge sont `SHA1` et `SHA256`. Si vous n'incluez pas ce cookie, la CloudFront valeur par défaut est. `SHA1`

L'exemple suivant illustre les en-têtes `Set-Cookie` d'un cookie signé quand vous utilisez le nom de domaine associé à votre distribution dans les URL de vos fichiers :

```
Set-Cookie: CloudFront-Expires=1426500000; Domain=d111111abcdef8.cloudfront.net; Path=/
images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=yXrSIgyQoeE4FBI4eMKF6ho~CA8_;
 Domain=d111111abcdef8.cloudfront.net; Path=/images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F;
 Domain=d111111abcdef8.cloudfront.net; Path=/images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Hash-Algorithm=SHA256; Domain=d111111abcdef8.cloudfront.net;
 Path=/images/*; Secure; HttpOnly
```

L'exemple suivant illustre les en-têtes `Set-Cookie` d'un cookie signé quand vous utilisez le nom de domaine alternatif example.org dans les URL de vos fichiers :

```
Set-Cookie: CloudFront-Expires=1426500000; Domain=example.org; Path=/images/*; Secure;
 HttpOnly
Set-Cookie: CloudFront-Signature=yXrSIgyQoeE4FBI4eMKF6ho~CA8_; Domain=example.org;
 Path=/images/*; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F; Domain=example.org; Path=/images/*;
 Secure; HttpOnly
Set-Cookie: CloudFront-Hash-Algorithm=SHA256; Domain=example.org; Path=/images/*;
 Secure; HttpOnly
```

Si vous souhaitez utiliser un nom de domaine alternatif tel qu'example.com dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez l'attribut `Domain` ou non. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence de tous les paramètres de distribution.

Création d'une signature pour un cookie signé qui utilise une politique prédéfinie

Pour créer la signature pour un cookie signé qui utilise une politique prédéfinie, suivez les procédures suivantes.

Rubriques

- Création d'une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie
- Signature d'une déclaration de politique pour créer une signature pour un cookie signé qui utilise une politique prédéfinie

Création d'une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie

Lorsque vous définissez un cookie signé qui utilise une politique prédéfinie, l'attribut `CloudFront-Signature` est une version hachée et signée d'une déclaration de politique. Pour les cookies signés

qui utilisent une politique prédéfinie, vous n'incluez pas la déclaration de politique dans l'en-tête `Set-Cookie`, comme vous le faites pour les cookies signés qui utilisent une politique personnalisée. Pour créer l'a déclaration de politique, procédez comme suit.

Pour créer une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie

1. Construisez la déclaration de politique en utilisant le format JSON suivant et en utilisant UTF-8 le codage de caractères. Incluez la ponctuation et les autres valeurs littérales exactement comme spécifié. Pour plus d'informations sur les paramètres `Resource` et `DateLessThan`, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une politique prédéfinie pour les cookies signés.

   ```
   {
       "Statement": [
           {
               "Resource": "base URL or stream name",
               "Condition": {
                   "DateLessThan": {
                       "AWS:EpochTime": ending date and time in Unix time format and
    UTC
                   }
               }
           }
       ]
   }
   ```

2. Supprimez tous les espaces vides (tabulations et sauts de ligne inclus) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.

Valeurs que vous spécifiez dans la déclaration de politique d'une politique prédéfinie pour les cookies signés

Lorsque vous créez une déclaration de politique pour une politique prédéfinie, vous spécifiez les valeurs suivantes :

Ressource

L'URL de base incluant vos chaînes de requête, le cas échéant ; par exemple :

`https://d111111abcdef8.cloudfront.net/images/horizon.jpg?size=large&license=yes`

Vous ne pouvez spécifier qu'une seule valeur pour `Resource`.

Remarques :

- Protocole : la valeur doit commencer par `http://` ou `https://`.
- Paramètres de chaîne de requête : si vous n'avez aucun paramètre de chaîne de requête, omettez le point d'interrogation.
- Noms de domaine alternatifs : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL, vous devez le spécifier lorsque vous référencez le fichier dans votre page ou application web. Ne spécifiez pas l'URL Amazon S3 pour le fichier.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. N'entourez pas la valeur de points d'interrogation.

Par exemple, la date 16 mars 2015 10 h 00 UTC est convertie en 1426500000 au format horaire Unix.

Cette valeur doit correspondre à la valeur de l'attribut `CloudFront-Expires` de l'en-tête `Set-Cookie`. N'entourez pas la valeur de points d'interrogation.

Pour plus d'informations, consultez Quand CloudFront vérifie la date et l'heure d'expiration d'un cookie signé.

Exemple de déclaration de politique pour une politique prédéfinie

Lorsque vous utilisez l'exemple de déclaration de politique suivant dans un cookie signé, un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/horizon.jpg` jusqu'au 16 mars 2015 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/horizon.jpg?
size=large&license=yes",
            "Condition": {
                "DateLessThan": {
```

```
                    "AWS:EpochTime": 1426500000
                }
            }
        }
    ]
}
```

Signature d'une déclaration de politique pour créer une signature pour un cookie signé qui utilise une politique prédéfinie

Pour créer la valeur de l'attribut `CloudFront-Signature` d'un en-tête `Set-Cookie`, vous hachez et signez la déclaration de politique que vous avez créée dans Pour créer une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez les rubriques suivantes :

- Utilisation d'une commande Linux et OpenSSL pour le chiffrement et l'encodage en base64
- Exemples de code pour la création de la signature d'une URL signée

> **Note**
>
> Les exemples liés sont utilisés SHA-1 par défaut. Pour l'utiliser à la SHA-256 place, remplacez `sha1` par `sha256` dans les commandes OpenSSL et incluez le `CloudFront-Hash-Algorithm` cookie avec une valeur de. `SHA256`

Pour créer une signature pour un cookie signé qui utilise une politique prédéfinie

1. Utilisez la fonction de SHA-256 hachage SHA-1 or et RSA pour hacher et signer la déclaration de politique que vous avez créée dans la procédurePour créer une déclaration de politique pour un cookie signé qui utilise une politique prédéfinie. Utilisez la version de la déclaration de politique qui n'inclut plus d'espaces vides.

   Si vous utilisez SHA-256, vous devez inclure le `CloudFront-Hash-Algorithm` cookie d'une valeur de`SHA256`.

   Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

> **Note**
>
> La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (tabulations et sauts de ligne inclus) de la chaîne hachée et signée.
3. Base64-encode la chaîne utilisant le codage MIME base64. Pour plus d'informations, consultez la Section 6.8, Base64 Content-Transfer-Encoding de la RFC 2045, MIME (Multipurpose Internet Mail Extensions), première partie : Format des corps des messages Internet.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Incluez la valeur obtenue dans l'en-tête `Set-Cookie` de la paire nom-valeur `CloudFront-Signature`. Puis retournez à Pour définir un cookie signé à l'aide d'une politique prédéfinie pour ajouter l'en-tête `Set-Cookie` de `CloudFront-Key-Pair-Id`.

Définition de cookies signés utilisant une politique personnalisée

Pour définir un cookie signé qui utilise une politique personnalisée, effectuez la procédure suivante.

Pour définir un cookie signé utilisant une politique personnalisée

1. Si vous utilisez .NET ou Java pour créer des URL signées et si vous n'avez pas reformaté la clé privée de votre paire de clés du format par défaut .pem en un format compatible avec .NET ou Java, procédez comme suit : Pour plus d'informations, consultez Reformatage de la clé privée (.NET et Java uniquement).
2. Programmez votre application pour envoyer trois `Set-Cookie` en-têtes aux spectateurs approuvés (ou quatre, si vous souhaitez spécifier un algorithme de hachage). Vous avez besoin

de trois `Set-Cookie` en-têtes car chaque `Set-Cookie` en-tête ne peut contenir qu'une seule paire nom-valeur, et un cookie CloudFront signé nécessite trois paires nom-valeur. Les paires nom-valeur sont : `CloudFront-Policy`, `CloudFront-Signature` et `CloudFront-Key-Pair-Id`. Vous pouvez éventuellement inclure une quatrième paire nom-valeur,`CloudFront-Hash-Algorithm`, pour spécifier l'algorithme de hachage utilisé pour la signature. Les valeurs doivent être présentes sur la visionneuse avant qu'un utilisateur ne puisse faire la requête d'un fichier dont vous voulez contrôler l'accès.

> **Note**
>
> En règle générale, nous recommandons d'exclure les attributs `Expires` et `Max-Age`. Cette exclusion conduit le navigateur à supprimer le cookie quand l'utilisateur ferme le navigateur, ce qui réduit la possibilité qu'une personne obtienne un accès non autorisé à votre contenu. Pour plus d'informations, consultez Prévention du mauvais usage des cookies signés.

Les noms des attributs de cookie sont sensibles à la casse.

Les sauts de ligne ne sont inclus que pour rendre les attributs plus lisibles.

```
Set-Cookie:
CloudFront-Policy=base64 encoded version of the policy statement;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly


Set-Cookie:
CloudFront-Signature=hashed and signed version of the policy statement;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly

Set-Cookie:
CloudFront-Key-Pair-Id=public key ID for the CloudFront public key whose
 corresponding private key you're using to generate the signature;
Domain=optional domain name;
```

```
Path=/optional directory path;
Secure;
HttpOnly

Set-Cookie:
CloudFront-Hash-Algorithm=SHA1 or SHA256;
Domain=optional domain name;
Path=/optional directory path;
Secure;
HttpOnly
```

(Facultatif) **`Domain`**

Nom de domaine du fichier demandé. Si vous ne spécifiez pas un attribut `Domain`, la valeur par défaut est le nom de domaine de l'URL et ne s'applique qu'au nom de domaine spécifié, non aux sous-domaines. Si vous spécifiez un attribut `Domain`, il s'applique aussi aux sous-domaines. Un point devant le nom de domaine (par exemple, `Domain=.example.com`) est facultatif. De plus, si vous spécifiez un attribut `Domain`, le nom de domaine de l'URL et la valeur de l'attribut `Domain` doivent correspondre.

Vous pouvez spécifier le nom de domaine CloudFront attribué à votre distribution, par exemple, d111111abcdef8.cloudfront.net, mais vous ne pouvez pas spécifier *.cloudfront.net pour le nom de domaine.

Si vous souhaitez utiliser un nom de domaine alternatif tel qu'example.com dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez l'attribut `Domain` ou non. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence de tous les paramètres de distribution.

(Facultatif) **`Path`**

Chemin d'accès du fichier demandé. Si vous ne spécifiez pas d'attribut `Path`, la valeur par défaut est le chemin d'accès de l'URL.

`Secure`

Nécessite que l'utilisateur chiffre les cookies avant d'envoyer une demande. Nous vous recommandons d'envoyer l'`Set-Cookie`en-tête via une connexion HTTPS pour vous assurer que les attributs des cookies sont protégés contre les attaques de type man-in-the-middle.

`HttpOnly`

Requiert que l'utilisateur n'envoie le cookie que dans les requêtes HTTP ou HTTPS.

`CloudFront-Policy`

Votre déclaration de politique au format JSON, avec suppression des espaces vide, puis encodage en base64. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique personnalisée.

La déclaration de politique contrôle l'accès accordé par un cookie signé à un utilisateur. Elle inclut les fichiers auxquels l'utilisateur peut accéder, une date et une heure d'expiration, une date et une heure (facultatif) auxquelles l'URL devient valide et une adresse IP (facultatif) ou une plage d'adresses IP autorisées à accéder au fichier.

`CloudFront-Signature`

Version hachée, signée et encodée en base 64 de la déclaration de politique JSON. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique personnalisée.

`CloudFront-Key-Pair-Id`

L'ID d'une clé CloudFront publique, par exemple`K2JCJMDEHXQW5F`. L'ID de clé publique indique CloudFront la clé publique à utiliser pour valider l'URL signée. CloudFrontcompare les informations de la signature à celles de la déclaration de politique pour vérifier que l'URL n'a pas été falsifiée.

Cette clé publique doit appartenir à un groupe de clés qui est un signataire approuvé dans la distribution. Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.

`CloudFront-Hash-Algorithm`

(Facultatif) Algorithme de hachage utilisé pour créer la signature. Les valeurs prises en charge sont `SHA1` et `SHA256`. Si vous n'incluez pas ce cookie, la CloudFront valeur par défaut est. `SHA1`

Exemples d'en-têtes **`Set-Cookie`** pour les politiques personnalisées

Consultez les exemples de paires d'en-têtes `Set-Cookie` suivants.

Si vous souhaitez utiliser un nom de domaine alternatif tel qu'example.org dans les URL, vous devez ajouter le nom de domaine alternatif à votre distribution, que vous spécifiiez l'attribut `Domain` ou non. Pour plus d'informations, consultez Noms de domaine alternatifs (CNAME) dans la rubrique Référence de tous les paramètres de distribution.

Example Exemple 1

Vous pouvez utiliser les en-têtes `Set-Cookie` d'un cookie signé quand vous utilisez le nom de domaine associé à votre distribution dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_;
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F;
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Hash-Algorithm=SHA256; Domain=d111111abcdef8.cloudfront.net;
 Path=/; Secure; HttpOnly
```

Example Exemple 2

Vous pouvez utiliser les en-têtes `Set-Cookie` d'un cookie signé quand vous utilisez un nom de domaine alternatif (example.org) dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=example.org; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_; Domain=example.org;
 Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F; Domain=example.org; Path=/; Secure;
 HttpOnly
Set-Cookie: CloudFront-Hash-Algorithm=SHA256; Domain=example.org; Path=/; Secure;
 HttpOnly
```

Example Exemple 3

Vous pouvez utiliser les paires d'en-têtes `Set-Cookie` d'une demande signée quand vous utilisez le nom de domaine associé à votre distribution dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_;
 Domain=d111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F;
 Domain=dd111111abcdef8.cloudfront.net; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Hash-Algorithm=SHA256; Domain=d111111abcdef8.cloudfront.net;
 Path=/; Secure; HttpOnly
```

Example Exemple 4

Vous pouvez utiliser les paires d'en-têtes `Set-Cookie` d'une demande signée quand vous utilisez un nom de domaine alternatif (example.org) associé à votre distribution dans les URL de vos fichiers.

```
Set-Cookie: CloudFront-
Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cDovL2QxMTExMTFhYmNkZWY4LmNsb3VkZnJvbnQubmV0L2dh
 Domain=example.org; Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Signature=dtKhpJ3aUYxqDIwepczPiDb9NXQ_; Domain=example.org;
 Path=/; Secure; HttpOnly
Set-Cookie: CloudFront-Key-Pair-Id=K2JCJMDEHXQW5F; Domain=example.org; Path=/; Secure;
 HttpOnly
Set-Cookie: CloudFront-Hash-Algorithm=SHA256; Domain=example.org; Path=/; Secure;
 HttpOnly
```

Création d'une déclaration de politique pour un cookie signé qui utilise une politique personnalisée

Pour créer une déclaration de politique pour une politique personnalisée, effectuez la procédure suivante. Pour obtenir des exemples de déclaration de politique qui contrôlent l'accès aux fichiers de différentes façons, consultez Exemple d'une déclaration de politique pour un cookie signé qui utilise une politique personnalisée.

Pour créer la déclaration de politique d'un cookie signé qui utilise une politique personnalisée

1. Construisez la déclaration de politique à l'aide du format JSON suivant.

```
{
    "Statement": [
        {
            "Resource": "URL of the file",
            "Condition": {
```

```
                "DateLessThan": {
                    "AWS:EpochTime":required ending date and time in Unix time
 format and UTC
                },
                "DateGreaterThan": {
                    "AWS:EpochTime":optional beginning date and time in Unix time
 format and UTC
                },
                "IpAddress": {
                    "AWS:SourceIp": "optional IP address"
                }
            }
        }
    ]
}
```

Remarques :

- Vous pouvez inclure une seule instruction.
- Utilisez UTF-8 le codage des caractères.
- Incluez la ponctuation et les noms de paramètre exactement comme spécifié. Les abréviations ne sont pas acceptées pour les noms de paramètre.
- L'ordre des paramètres de la section `Condition` n'importe pas.
- Pour plus d'informations sur les valeurs de `Resource`, `DateLessThan`, `DateGreaterThan` et `IpAddress`, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés.

2. Supprimez tous les espaces vides (tabulations et sauts de ligne inclus) de la déclaration de politique. Il se peut que vous ayez à inclure des caractères d'échappement dans la chaîne du code d'application.
3. Base64-encode la déclaration de politique utilisant le codage MIME base64. Pour plus d'informations, consultez la Section 6.8, Base64 Content-Transfer-Encoding de la RFC 2045, MIME (Multipurpose Internet Mail Extensions), première partie : Format des corps des messages Internet.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Incluez la valeur obtenue dans votre en-tête `Set-Cookie` après `CloudFront-Policy=`.
6. Créez une signature pour l'en-tête `Set-Cookie` de `CloudFront-Signature` en hachant, signant et encodant en base64 la déclaration de politique. Pour plus d'informations, consultez Création d'une signature pour un cookie signé qui utilise une politique personnalisée.

Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés

Lorsque vous créez une déclaration de politique pour une politique personnalisée, vous spécifiez les valeurs suivantes.

Ressource

L'URL de base incluant vos chaînes de requête, le cas échéant :

```
https://d111111abcdef8.cloudfront.net/images/horizon.jpg?
size=large&license=yes
```

> **Important**
>
> Si vous omettez le paramètre `Resource`, les utilisateurs peuvent accéder à tous les fichiers associés à une distribution elle-même associée à la paire de clés que vous utilisez pour créer l'URL signée.

Vous ne pouvez spécifier qu'une seule valeur pour `Resource`.

Remarques :

- Protocole : la valeur doit commencer par `http://` ou `https://`.

- Paramètres de chaîne de requête : si vous n'avez aucun paramètre de chaîne de requête, omettez le point d'interrogation.
- Caractères génériques : vous pouvez utiliser à tout moment dans la chaîne, le caractère générique qui correspond à zéro caractère ou plus (*) ou celui qui correspond exactement à un seul caractère (?). Par exemple, la valeur :

  ```
  https://d111111abcdef8.cloudfront.net/*game_download.zip*
  ```

  inclut (par exemple) les fichiers suivants :

  - `https://d111111abcdef8.cloudfront.net/game_download.zip`
  - `https://d111111abcdef8.cloudfront.net/example_game_download.zip?license=yes`
  - `https://d111111abcdef8.cloudfront.net/test_game_download.zip?license=temp`

  Un caractère codé en pourcentage dans l'URL de la demande (par exemple `%3B` pour`;`, pour ou `%3F` `%23` pour ?#) est traité comme une donnée et non comme un délimiteur d'URL. Par exemple, un caractère générique ne peut pas correspondre à un point-virgule littéral (`;`), mais il peut correspondre à la forme codée (). `%3B` Pour plus d'informations, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une URL signée utilisant une politique personnalisée.
- Noms de domaine alternatifs : si vous spécifiez un nom de domaine alternatif (CNAME) dans l'URL, vous devez le spécifier lorsque vous référencez le fichier dans votre page ou application web. Ne spécifiez pas l'URL Amazon S3 pour le fichier.

DateLessThan

Date et heure d'expiration de l'URL au format horaire Unix (en secondes) et en heure UTC. N'entourez pas la valeur de points d'interrogation.

Par exemple, la date 16 mars 2015 10 h 00 UTC est convertie en 1426500000 au format horaire Unix.

Pour plus d'informations, consultez Quand CloudFront vérifie la date et l'heure d'expiration d'un cookie signé.

DateGreaterThan (Facultatif)

(Facultatif) Date et heure de début de l'URL au format horaire Unix (en secondes) et en heure UTC. Les utilisateurs ne sont pas autorisés à accéder au fichier avant la date et l'heure spécifiées. N'entourez pas la valeur de points d'interrogation.

IpAddress (Facultatif)

Adresse IP du client formulant la demande GET. Remarques :

- Pour autoriser une adresse IP à accéder au fichier, omettez le paramètre `IpAddress`.
- Vous pouvez spécifier une adresse IP ou une plage d'adresses IP. Par exemple, vous pouvez définir la politique pour autoriser l'accès si l'adresse IP du client figure dans l'une des deux plages distinctes.
- Pour autoriser l'accès depuis une seule adresse IP, vous spécifiez :

  `"`*`IPv4 IP address`*`/32"`
- Vous devez spécifier les plages d'adresses IP selon le format IPv4 CIDR standard (par exemple, `192.0.2.0/24`). Pour plus d'informations, consultez la RFC 4632, Inter-domain Routage sans classe (CIDR) : le plan d'attribution et d'agrégation d'adresses Internet,. https://tools.ietf.org/html/rfc4632

  > **Important**
  >
  > Les adresses IP au format IPv6, telles que 2001:0db8:85a3::8a2e:0370:7334, ne sont pas prises en charge.

  Si vous utilisez une politique personnalisée qui inclut `IpAddress`, n'activez pas IPv6 pour la distribution. Si vous souhaitez limiter l'accès à un contenu spécifique par adresse IP et prendre en charge les requêtes IPv6 pour les autres contenus, vous pouvez créer deux distributions. Pour plus d'informations, consultez Activation d'IPv6 (demandes des utilisateurs) dans la rubrique Référence de tous les paramètres de distribution.

Exemple d'une déclaration de politique pour un cookie signé qui utilise une politique personnalisée

Les exemples suivants de déclaration de politique montrent comment accéder à un fichier spécifique, à tous les objets d'un répertoire ou à tous les fichiers associés à un ID de paire de clés. Les exemples montrent aussi comment contrôler l'accès depuis une adresse IP individuelle ou une plage

d'adresses IP, et comment empêcher les utilisateurs d'employer le cookie signé au-delà d'une date et heure spécifiées.

Si vous copiez et collez l'un de ces exemples, supprimez les espaces vides (y compris les tabulations et les sauts de ligne), remplacez les valeurs par vos propres valeurs et incluez un caractère de saut de ligne après l'accolade fermante (}).

Pour plus d'informations, consultez Valeurs que vous spécifiez dans la déclaration de politique d'une politique personnalisée pour les cookies signés.

Rubriques

- Exemple de déclaration de politique : accès à un fichier à partir d'une plage d'adresses IP
- Exemple de déclaration de politique : accès à tous les fichiers d'un répertoire à partir d'une plage d'adresses IP
- Exemple de déclaration de politique : accès à tous les fichiers associés à un ID de paire de clés à partir d'une adresse IP

Exemple de déclaration de politique : accès à un fichier à partir d'une plage d'adresses IP

L'exemple suivant de politique personnalisée dans un cookie signé spécifie qu'un utilisateur peut accéder au fichier `https://d111111abcdef8.cloudfront.net/game_download.zip` à partir des adresses IP de la plage `192.0.2.0/24` jusqu'au 1er janvier 2023 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/game_download.zip",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Exemple de déclaration de politique : accès à tous les fichiers d'un répertoire à partir d'une plage d'adresses IP

Avec l'exemple de politique personnalisée suivant, vous pouvez créer des cookies signés pour n'importe quel fichier du `training` répertoire, comme indiqué par le caractère générique * dans le `Resource` paramètre. Les utilisateurs peuvent accéder au fichier depuis une adresse IP de la plage `192.0.2.0/24` jusqu'au 1er janvier 2013 10 h 00 UTC :

```
{
    "Statement": [
        {
            "Resource": "https://d111111abcdef8.cloudfront.net/training/*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.0/24"
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767290400
                }
            }
        }
    ]
}
```

Chaque cookie signé dans lequel vous utilisez cette politique inclut une URL de base qui identifie un fichier spécifique ; par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Exemple de déclaration de politique : accès à tous les fichiers associés à un ID de paire de clés à partir d'une adresse IP

Avec l'exemple de politique personnalisée suivant, vous pouvez définir des cookies signés pour n'importe quel fichier associé à une distribution, comme indiqué par le caractère générique * dans le `Resource` paramètre. L'utilisateur doit employer l'adresse IP `192.0.2.10/32`. (La valeur `192.0.2.10/32` en notation CIDR fait référence à une seule adresse IP, `192.0.2.10`.) Les fichiers ne sont disponibles qu'entre le 1er janvier 2013 10 h 00 UTC et le 2 janvier 2013 10 h 00 UTC :

```
{
    "Statement": [
        {
```

```
            "Resource": "https://*",
            "Condition": {
                "IpAddress": {
                    "AWS:SourceIp": "192.0.2.10/32"
                },
                "DateGreaterThan": {
                    "AWS:EpochTime": 1767290400
                },
                "DateLessThan": {
                    "AWS:EpochTime": 1767376800
                }
            }
        }
    ]
}
```

Chaque cookie signé dans lequel vous utilisez cette politique inclut une URL de base qui identifie un fichier spécifique dans une CloudFront distribution spécifique, par exemple :

`https://d111111abcdef8.cloudfront.net/training/orientation.pdf`

Le cookie signé inclut aussi un ID de paire de clés, qui doit être associé à un groupe de clés approuvé de la distribution (d111111abcdef8.cloudfront.net) que vous spécifiez dans l'URL de base.

Création d'une signature pour un cookie signé qui utilise une politique personnalisée

La signature d'un cookie signé utilisant une politique personnalisée est une version hachée, signée et encodée en base64 de la déclaration de politique.

Pour plus d'informations et d'exemples sur la façon de hacher, signer et encoder la déclaration de politique, consultez :

- Utilisation d'une commande Linux et OpenSSL pour le chiffrement et l'encodage en base64
- Exemples de code pour la création de la signature d'une URL signée

> **Note**
>
> Les exemples liés sont utilisés SHA-1 par défaut. Pour l'utiliser à la SHA-256 place, remplacez `sha1` par `sha256` dans les commandes OpenSSL et incluez le `CloudFront-Hash-Algorithm` cookie avec une valeur de. `SHA256`

Pour créer une signature pour un cookie signé en utilisant une politique personnalisée

1. Utilisez la fonction de SHA-256 hachage SHA-1 or et RSA pour hacher et signer la déclaration de politique JSON que vous avez créée au cours de la procédurePour créer la déclaration de politique d'une URL signée qui utilise une politique personnalisée. Utilisez la version de la déclaration de politique qui n'inclut plus d'espaces vides, mais qui n'a pas encore été encodée en base64.

   Si vous utilisez SHA-256, vous devez inclure le `CloudFront-Hash-Algorithm` cookie d'une valeur de`SHA256`.

   Pour la clé privée requise par la fonction de hachage, utilisez une clé privée dont la clé publique se trouve dans un groupe de clés approuvé actif pour la distribution.

   > **Note**
   >
   > La méthode que vous utilisez pour hacher et signer la déclaration de politique dépend du langage de programmation et de la plateforme. Pour un exemple de code, consultez Exemples de code pour la création de la signature d'une URL signée.

2. Supprimez les espaces vides (tabulations et sauts de ligne inclus) de la chaîne hachée et signée.
3. Base64-encode la chaîne utilisant le codage MIME base64. Pour plus d'informations, consultez la Section 6.8, Base64 Content-Transfer-Encoding de la RFC 2045, MIME (Multipurpose Internet Mail Extensions), première partie : Format des corps des messages Internet.
4. Remplacez les caractères non valides d'une chaîne de requête d'URL par les caractères valides. Le tableau suivant répertorie les caractères valides et non valides.

Remplacer ces caractères non valides	Par ces caractères valides
+	- (trait d'union)
=	_ (soulignement)
/	~ (tilde)

5. Incluez la valeur obtenue dans l'en-tête `Set-Cookie` de la paire nom-valeur `CloudFront-Signature=`, et retournez à Pour définir un cookie signé utilisant une politique personnalisée pour ajouter l'en-tête `Set-Cookie` de `CloudFront-Key-Pair-Id`.

Création de cookies signés avec PHP

L'exemple de code suivant est similaire à celui indiqué dans Créer une signature d'URL avec PHP, puisqu'il génère un lien vers une vidéo. Cependant, au lieu de signer l'URL dans le code, cet exemple signe les cookies avec la fonction `create_signed_cookies()`. Le lecteur côté client utilise les cookies pour authentifier chaque demande adressée à la distribution. CloudFront

Cette approche est utile pour diffuser du contenu en continu, comme le HTTP Live Streaming (HLS) ou le Dynamic Adaptive Streaming over HTTP (DASH), où le client doit envoyer plusieurs demandes pour récupérer le manifeste, les segments et les ressources associées à la lecture. En utilisant des cookies signés, le client peut authentifier chaque demande sans avoir à générer une nouvelle URL signée pour chaque segment.

> **Note**
>
> - La création d'une signature d'URL n'est qu'une partie du processus d'offre d'un contenu privé avec des cookies signés. Pour plus d'informations, consultez Utilisation de cookies signés.

Rubriques

- Créez le RSA SHA-1 ou la signature SHA-256
- Création des cookies signés
- Code complet

Les sections suivantes décomposent l'exemple de code en plusieurs parties. Vous trouverez l'exemple de code complet ci-dessous.

Créez le RSA SHA-1 ou la signature SHA-256

Cet exemple de code effectue les opérations suivantes :

1. La fonction `rsa_sha1_sign` hache et signe la déclaration de politique en utilisant SHA-1. Pour l'utiliser à la SHA-256 place, utilisez la fonction rsa_sha256_sign illustrée ci-dessous. Les arguments requis sont une déclaration de politique et la clé privée qui correspond à une clé publique qui se trouve dans un groupe de clés approuvé pour votre distribution.
2. Ensuite, la `url_safe_base64_encode` fonction crée une URL-safe version de la signature.

```
function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid);
    openssl_free_key($pkeyid);
    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}
```

La fonction suivante utilise SHA-256 au lieu de SHA-1 :

```
function rsa_sha256_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid, OPENSSL_ALGO_SHA256);
    openssl_free_key($pkeyid);
    return $signature;
}
```

La `rsa_sha256_sign` fonction est la même que`rsa_sha1_sign`, sauf qu'elle passe `OPENSSL_ALGO_SHA256` à`openssl_sign`. Lorsque vous l'utilisez SHA-256, incluez le `CloudFront-Hash-Algorithm` cookie d'une valeur de`SHA256`.

Création des cookies signés

Le code suivant construit et crée les cookies signés à l'aide des attributs de cookie suivants : `CloudFront-Expires`CloudFront-Signature, `CloudFront-Key-Pair-Id` et`CloudFront-Hash-Algorithm`. Le code utilise une politique personnalisée.

```
function create_signed_cookies($resource, $private_key_filename, $key_pair_id,
 $expires, $client_ip = null, $hash_algorithm = 'SHA1') {
    $policy = array(
        'Statement' => array(
            array(
                'Resource' => $resource,
                'Condition' => array(
                    'DateLessThan' => array('AWS:EpochTime' => $expires)
                )
            )
        )
    );

    if ($client_ip) {
        $policy['Statement'][0]['Condition']['IpAddress'] = array('AWS:SourceIp' =>
 $client_ip . '/32');
    }

    $policy = json_encode($policy);
    $encoded_policy = url_safe_base64_encode($policy);
    if ($hash_algorithm === 'SHA256') {
        $signature = rsa_sha256_sign($policy, $private_key_filename);
    } else {
        $signature = rsa_sha1_sign($policy, $private_key_filename);
    }
    $encoded_signature = url_safe_base64_encode($signature);

    $cookies = array(
        'CloudFront-Policy' => $encoded_policy,
        'CloudFront-Signature' => $encoded_signature,
        'CloudFront-Key-Pair-Id' => $key_pair_id
    );

    if ($hash_algorithm === 'SHA256') {
        $cookies['CloudFront-Hash-Algorithm'] = 'SHA256';
    }
```

```
    return $cookies;
}
```

Pour plus d'informations, consultez Définition de cookies signés utilisant une politique personnalisée.

Code complet

L'exemple de code suivant fournit une démonstration complète de la création de cookies CloudFront signés avec PHP. Vous pouvez télécharger l'exemple complet depuis le fichier demo-php.zip.

Dans l'exemple suivant, vous pouvez modifier l'élément `$policy Condition` pour autoriser à la fois des plages d'adresses IPv4 et IPv6. Consultez par exemple Utilisation d'adresses IPv6 dans les politiques IAM dans le Guide de l'utilisateur Amazon Simple Storage Service.

```
<?php

function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid);
    openssl_free_key($pkeyid);
    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}

function rsa_sha256_sign($policy, $private_key_filename) {
    $signature = "";
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);
    openssl_sign($policy, $signature, $pkeyid, OPENSSL_ALGO_SHA256);
    openssl_free_key($pkeyid);
```

```
    return $signature;
}

function create_signed_cookies($resource, $private_key_filename, $key_pair_id,
 $expires, $client_ip = null, $hash_algorithm = 'SHA1') {
    $policy = array(
        'Statement' => array(
            array(
                'Resource' => $resource,
                'Condition' => array(
                    'DateLessThan' => array('AWS:EpochTime' => $expires)
                )
            )
        )
    );

    if ($client_ip) {
        $policy['Statement'][0]['Condition']['IpAddress'] = array('AWS:SourceIp' =>
 $client_ip . '/32');
    }

    $policy = json_encode($policy);
    $encoded_policy = url_safe_base64_encode($policy);
    if ($hash_algorithm === 'SHA256') {
        $signature = rsa_sha256_sign($policy, $private_key_filename);
    } else {
        $signature = rsa_sha1_sign($policy, $private_key_filename);
    }
    $encoded_signature = url_safe_base64_encode($signature);

    $cookies = array(
        'CloudFront-Policy' => $encoded_policy,
        'CloudFront-Signature' => $encoded_signature,
        'CloudFront-Key-Pair-Id' => $key_pair_id
    );

    if ($hash_algorithm === 'SHA256') {
        $cookies['CloudFront-Hash-Algorithm'] = 'SHA256';
    }

    return $cookies;
}
```

```
$private_key_filename = '/home/test/secure/example-priv-key.pem';
$key_pair_id = 'K2JCJMDEHXQW5F';
$base_url = 'https://d1234.cloudfront.net';

$expires = time() + 3600; // 1 hour from now

// Get the viewer real IP from the x-forward-for header as $_SERVER['REMOTE_ADDR']
 will return viewer facing IP. An alternative option is to use CloudFront-Viewer-
Address header. Note that this header is a trusted CloudFront immutable header. Example
 format: IP:PORT ("CloudFront-Viewer-Address": "1.2.3.4:12345")
$client_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];


// For HLS manifest and segments (using wildcard)
$hls_resource = $base_url . '/sign/*';
$signed_cookies = create_signed_cookies($hls_resource, $private_key_filename,
 $key_pair_id, $expires, $client_ip, 'SHA256');

// Set the cookies
$cookie_domain = parse_url($base_url, PHP_URL_HOST);
foreach ($signed_cookies as $name => $value) {
    setcookie($name, $value, $expires, '/', $cookie_domain, true, true);
}

?>

<!DOCTYPE html>
<html>
<head>
    <title>CloudFront Signed HLS Stream with Cookies</title>
</head>
<body>
    <h1>Amazon CloudFront Signed HLS Stream with Cookies</h1>
    <h2>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?> only viewable by IP
 <?php echo $client_ip; ?></h2>

    <div id='hls-video'>
        <video id="video" width="640" height="360" controls></video>
    </div>

    <script src="https://cdn.jsdelivr.net/npm/hls.js@latest"></script>
    <script>
        var video = document.getElementById('video');
```

```
        var manifestUrl = '<?php echo $base_url; ?>/sign/manifest.m3u8';

        if (Hls.isSupported()) {
            var hls = new Hls();
            hls.loadSource(manifestUrl);
            hls.attachMedia(video);
        }
        else if (video.canPlayType('application/vnd.apple.mpegurl')) {
            video.src = manifestUrl;
        }
    </script>
</body>
</html>
```

Au lieu d'utiliser des cookies signés, vous pouvez utiliser des URL signées. Pour plus d'informations, consultez Créer une signature d'URL avec PHP.

Utilisation d'une commande Linux et OpenSSL pour le chiffrement et l'encodage en base64

Vous pouvez utiliser la commande de ligne de commande Linux suivante et OpenSSL pour hacher et signer la déclaration de politique, encoder la signature en base64 et remplacer les caractères non valides des paramètres de la chaîne de requête de l'URL par des caractères valides.

Pour plus d'informations sur OpenSSL, rendez-vous sur https://www.openssl.org.

SHA-1 (par défaut) :

```
cat policy | tr -d "\n" | tr -d " \t\n\r" | openssl sha1 -sign private_key.pem |
 openssl base64 -A | tr -- '+=/' '-_~'
```

SHA-256:

```
cat policy | tr -d "\n" | tr -d " \t\n\r" | openssl sha256 -sign private_key.pem |
 openssl base64 -A | tr -- '+=/' '-_~'
```

Dans la commande précédente :

- `cat` lit le fichier `policy`.
- `tr -d "\n" | tr -d " \t\n\r"` supprime les espaces vides et le caractère de saut de ligne qui ont été ajoutés par `cat`.

- OpenSSL hache le fichier à l'aide de SHA-1 (ou SHA-256) et le signe à l'aide du fichier de clé privée. `private_key.pem` La signature de clé privée peut être RSA 2048 ou ECDSA 256. Si vous utilisez SHA-256, incluez le paramètre de `Hash-Algorithm=SHA256` requête dans l'URL signée ou le `CloudFront-Hash-Algorithm=SHA256` cookie pour les cookies signés.
- OpenSSL encode en base64 la déclaration de politique hachée et signée.
- `tr`remplace les caractères qui ne sont pas valides dans les paramètres de chaîne de requête URL par des caractères valides.

Pour d'autres exemples de code illustrant la création d'une signature, consultez Exemples de code pour la création de la signature d'une URL signée.

Exemples de code pour la création de la signature d'une URL signée

Cette section inclut des exemples d'application téléchargeables qui montrent comment créer des signatures pour les URL signées. Les exemples sont disponibles en Perl, PHP, C# et Java. Vous pouvez utiliser l'un des exemples pour créer des URL signées. Le script Perl s'exécute sur les plateformes Linux et MacOS. L'exemple PHP fonctionne sur n'importe quel serveur qui exécute PHP. L'exemple C# utilise le .NET Framework.

Les exemples de cette section permettent de SHA-1 hacher et de signer la déclaration de politique. Vous pouvez également utiliser SHA-256. Pour l'utiliser SHA-256, mettez à jour l'algorithme de hachage dans la fonction de signature (par exemple, remplacez-le `sha1` par `sha256` dans les appels OpenSSL ou utilisez la SHA-256 constante équivalente dans la bibliothèque cryptographique de votre langue). Lorsque vous utilisez SHA-256, incluez le paramètre de `Hash-Algorithm=SHA256` requête dans l'URL signée.

Pour un exemple de code dans JavaScript (Node.js), consultez la section Création d'URL CloudFront signées Amazon Node.js sur le blog des AWS développeurs.

Pour un exemple de code en Python, voir Générer une URL signée pour Amazon CloudFront dans la référence d'API du AWS SDK pour Python (Boto3) et cet exemple de code dans le référentiel Boto3. GitHub

Rubriques

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework

- Créer une signature d’URL avec Java

Créer une signature d’URL avec Perl

Cette section inclut un script Perl pour les Linux/Mac plateformes que vous pouvez utiliser pour créer la signature d'un contenu privé. Pour créer la signature, exécutez le script avec des arguments de ligne de commande qui spécifient l' CloudFront URL, le chemin d'accès à la clé privée du signataire, l'ID de clé et une date d'expiration pour l'URL. L’outil peut aussi décoder les URL signées.

> **Remarques**
>
> - La création d’une signature d’URL n’est qu’une partie du processus d’offre d’un contenu privé avec une URL signée. Pour plus d’informations sur la totalité du processus, consultez Utilisation des URL signées.
> - Dans la commande de signature, notez qu'`sha1`elle peut être remplacée par `sha256` dans l'`openssl dgst`appel.

Rubriques

- Source du script Perl pour la création d’une URL signée

Source du script Perl pour la création d’une URL signée

Le code source Perl suivant peut être utilisé pour créer une URL signée pour CloudFront. Les commentaires du code incluent les informations sur les fonctions et les commutateurs de ligne de commande de l’outil.

```
#!/usr/bin/perl -w

# Copyright 2008 Amazon Technologies, Inc.  Licensed under the Apache License, Version
 2.0 (the "License");
# you may not use this file except in compliance with the License. You may obtain a
 copy of the License at:
#
# https://aws.amazon.com/apache2.0
#
# This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
 KIND, either express or implied.
```

```
# See the License for the specific language governing permissions and limitations under
 the License.

=head1 cfsign.pl

cfsign.pl - A tool to generate and verify Amazon CloudFront signed URLs

=head1 SYNOPSIS

This script uses an existing RSA key pair to sign and verify Amazon CloudFront signed
 URLs

View the script source for details as to which CPAN packages are required beforehand.

For help, try:

cfsign.pl --help

URL signing examples:

cfsign.pl --action encode --url https://images.my-website.com/gallery1.zip --policy
 sample_policy.json --private-key privkey.pem --key-pair-id mykey

cfsign.pl --action encode --url https://images.my-website.com/gallery1.zip --expires
 1257439868 --private-key privkey.pem --key-pair-id mykey

URL decode example:

cfsign.pl --action decode --url "http//mydist.cloudfront.net/?Signature=AGO-
PgxkYo99MkJFHvjfGXjG1QDEXeaDb4Qtzmy85wqyJjK7eKojQWa4BCRcow__&Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc29
Pair-Id=mykey"


To generate an RSA key pair, you can use openssl and the following commands:

# Generate a 2048 bit key pair
openssl genrsa -out private-key.pem 2048
openssl rsa -in private-key.pem -pubout -out public-key.pem


=head1 OPTIONS

=over 8
```

```
=item B<--help>

Print a help message and exits.

=item B<--action> [action]

The action to execute.  action can be one of:

  encode - Generate a signed URL (using a canned policy or a user policy)
  decode - Decode a signed URL

=item B<--url>

The URL to en/decode

=item B<--stream>

The stream to en/decode

=item B<--private-key>

The path to your private key.

=item B<--key-pair-id>

The key pair identifier.

=item B<--policy>

The CloudFront policy document.

=item B<--expires>

The Unix epoch time when the URL is to expire. If both this option and
the --policy option are specified, --policy will be used. Otherwise, this
option alone will use a canned policy.

=back

=cut

use strict;
use warnings;
```

```
# you might need to use CPAN to get these modules.
# run perl -MCPAN -e "install <module>" to get them.
# The openssl command line will also need to be in your $PATH.
use File::Temp qw/tempfile/;
use File::Slurp;
use Getopt::Long;
use IPC::Open2;
use MIME::Base64 qw(encode_base64 decode_base64);
use Pod::Usage;
use URI;

my $CANNED_POLICY
    = '{"Statement":[{"Resource":"<RESOURCE>","Condition":{"DateLessThan":
{"AWS:EpochTime":<EXPIRES>}}}]}';

my $POLICY_PARAM      = "Policy";
my $EXPIRES_PARAM     = "Expires";
my $SIGNATURE_PARAM   = "Signature";
my $KEY_PAIR_ID_PARAM = "Key-Pair-Id";

my $verbose = 0;
my $policy_filename = "";
my $expires_epoch = 0;
my $action = "";
my $help = 0;
my $key_pair_id = "";
my $url = "";
my $stream = "";
my $private_key_filename = "";

my $result = GetOptions("action=s"      => \$action,
                        "policy=s"      => \$policy_filename,
                        "expires=i"     => \$expires_epoch,
                        "private-key=s" => \$private_key_filename,
                        "key-pair-id=s" => \$key_pair_id,
                        "verbose"       => \$verbose,
                        "help"          => \$help,
                        "url=s"         => \$url,
                        "stream=s"      => \$stream,
                    );

if ($help or !$result) {
    pod2usage(1);
    exit;
```

```
}

if ($url eq "" and $stream eq "") {
    print STDERR "Must include a stream or a URL to encode or decode with the --stream
 or --url option\n";
    exit;
}

if ($url ne "" and $stream ne "") {
    print STDERR "Only one of --url and --stream may be specified\n";
    exit;
}

if ($url ne "" and !is_url_valid($url)) {
    exit;
}

if ($stream ne "") {
    exit unless is_stream_valid($stream);

    # The signing mechanism is identical, so from here on just pretend we're
    # dealing with a URL
    $url = $stream;
}

if ($action eq "encode") {
    # The encode action will generate a private content URL given a base URL,
    # a policy file (or an expires timestamp) and a key pair id parameter
    my $private_key;
    my $public_key;
    my $public_key_file;

    my $policy;
    if ($policy_filename eq "") {
        if ($expires_epoch == 0) {
            print STDERR "Must include policy filename with --policy argument or an
 expires" .
                         "time using --expires\n";
        }

        $policy = $CANNED_POLICY;
        $policy =~ s/<EXPIRES>/$expires_epoch/g;
        $policy =~ s/<RESOURCE>/$url/g;
    } else {
```

```
        if (! -e $policy_filename) {
            print STDERR "Policy file $policy_filename does not exist\n";
            exit;
        }
        $expires_epoch = 0; # ignore if set
        $policy = read_file($policy_filename);
    }

    if ($private_key_filename eq "") {
        print STDERR "You must specific the path to your private key file with --
private-key\n";
        exit;
    }

    if (! -e $private_key_filename) {
        print STDERR "Private key file $private_key_filename does not exist\n";
        exit;
    }

    if ($key_pair_id eq "") {
        print STDERR "You must specify a key pair id with --key-pair-id\n";
        exit;
    }

    my $encoded_policy = url_safe_base64_encode($policy);
    my $signature = rsa_sha1_sign($policy, $private_key_filename);
    my $encoded_signature = url_safe_base64_encode($signature);

    my $generated_url = create_url($url, $encoded_policy, $encoded_signature,
 $key_pair_id, $expires_epoch);


    if ($stream ne "") {
        print "Encoded stream (for use within a swf):\n" . $generated_url . "\n";
        print "Encoded and escaped stream (for use on a webpage):\n" .
 escape_url_for_webpage($generated_url) . "\n";
    } else {
        print "Encoded URL:\n" . $generated_url . "\n";
    }
} elsif ($action eq "decode") {
    my $decoded = decode_url($url);
    if (!$decoded) {
        print STDERR "Improperly formed URL\n";
        exit;
```

```
    }

    print_decoded_url($decoded);
} else {
    # No action specified, print help.  But only if this is run as a program (caller
 will be empty)
    pod2usage(1) unless caller();
}

# Decode a private content URL into its component parts
sub decode_url {
    my $url = shift;

    if ($url =~ /(.*)\?(.*)/) {
        my $base_url = $1;
        my $params = $2;

        my @unparsed_params = split(/&/, $params);
        my %params = ();
        foreach my $param (@unparsed_params) {
            my ($key, $val) = split(/=/, $param);
            $params{$key} = $val;
        }

        my $encoded_signature = "";
        if (exists $params{$SIGNATURE_PARAM}) {
            $encoded_signature = $params{"Signature"};
        } else {
            print STDERR "Missing Signature URL parameter\n";
            return 0;
        }

        my $encoded_policy = "";
        if (exists $params{$POLICY_PARAM}) {
            $encoded_policy = $params{$POLICY_PARAM};
        } else {
            if (!exists $params{$EXPIRES_PARAM}) {
                print STDERR "Either the Policy or Expires URL parameter needs to be
 specified\n";
                return 0;
            }

            my $expires = $params{$EXPIRES_PARAM};
```

```
            my $policy = $CANNED_POLICY;
            $policy =~ s/<EXPIRES>/$expires/g;

            my $url_without_cf_params = $url;
            $url_without_cf_params =~ s/$SIGNATURE_PARAM=[^&]*&?//g;
            $url_without_cf_params =~ s/$POLICY_PARAM=[^&]*&?//g;
            $url_without_cf_params =~ s/$EXPIRES_PARAM=[^&]*&?//g;
            $url_without_cf_params =~ s/$KEY_PAIR_ID_PARAM=[^&]*&?//g;

            if ($url_without_cf_params =~ /(.*)\?$/) {
                $url_without_cf_params = $1;
            }

            $policy =~ s/<RESOURCE>/$url_without_cf_params/g;

            $encoded_policy = url_safe_base64_encode($policy);
        }

        my $key = "";
        if (exists $params{$KEY_PAIR_ID_PARAM}) {
            $key = $params{$KEY_PAIR_ID_PARAM};
        } else {
            print STDERR "Missing $KEY_PAIR_ID_PARAM parameter\n";
            return 0;
        }

        my $policy = url_safe_base64_decode($encoded_policy);

        my %ret = ();
        $ret{"base_url"} = $base_url;
        $ret{"policy"} = $policy;
        $ret{"key"} = $key;

        return \%ret;
    } else {
        return 0;
    }
}

# Print a decoded URL out
sub print_decoded_url {
    my $decoded = shift;

    print "Base URL: \n" . $decoded->{"base_url"} . "\n";
```

```
    print "Policy: \n" . $decoded->{"policy"} . "\n";
    print "Key: \n" . $decoded->{"key"} . "\n";
}

# Encode a string with base 64 encoding and replace some invalid URL characters
sub url_safe_base64_encode {
    my ($value) = @_;

    my $result = encode_base64($value);
    $result =~ tr|+=/|-_~|;

    return $result;
}

# Decode a string with base 64 encoding.  URL-decode the string first
# followed by reversing any special character ("+=/") translation.
sub url_safe_base64_decode {
    my ($value) = @_;

    $value =~ s/%([0-9A-Fa-f]{2})/chr(hex($1))/eg;
    $value =~ tr|-_~|+=/|;

    my $result = decode_base64($value);

    return $result;
}

# Create a private content URL
sub create_url {
    my ($path, $policy, $signature, $key_pair_id, $expires) = @_;

    my $result;
    my $separator = $path =~ /\?/ ? '&' : '?';
    if ($expires) {
        $result = "$path$separator$EXPIRES_PARAM=$expires&$SIGNATURE_PARAM=$signature&
$KEY_PAIR_ID_PARAM=$key_pair_id";
    } else {
        $result = "$path$separator$POLICY_PARAM=$policy&$SIGNATURE_PARAM=$signature&
$KEY_PAIR_ID_PARAM=$key_pair_id";
    }
    $result =~ s/\n//g;

    return $result;
}
```

```
# Sign a document with given private key file.
# The first argument is the document to sign
# The second argument is the name of the private key file
sub rsa_sha1_sign {
    my ($to_sign, $pvkFile) = @_;
    print "openssl sha1 -sign $pvkFile $to_sign\n";

    return write_to_program($pvkFile, $to_sign);
}

# Helper function to write data to a program
sub write_to_program {
my ($keyfile, $data) = @_;
unlink "temp_policy.dat" if (-e "temp_policy.dat");
unlink "temp_sign.dat" if (-e "temp_sign.dat");

write_file("temp_policy.dat", $data);

system("openssl dgst -sha1 -sign \"$keyfile\" -out temp_sign.dat temp_policy.dat");

my $output = read_file("temp_sign.dat");

    return $output;
}

# Read a file into a string and return the string
sub read_file {
    my ($file) = @_;

    open(INFILE, "<$file") or die("Failed to open $file: $!");
    my $str = join('', <INFILE>);
    close INFILE;

    return $str;
}

sub is_url_valid {
    my ($url) = @_;

    # HTTP distributions start with http[s]:// and are the correct thing to sign
    if ($url =~ /^https?:\/\//) {
        return 1;
    } else {
```

```
        print STDERR "CloudFront requires absolute URLs for HTTP distributions\n";
        return 0;
    }
}

sub is_stream_valid {
    my ($stream) = @_;

    if ($stream =~ /^rtmp:\/\// or $stream =~ /^\/?cfx\/st/) {
        print STDERR "Streaming distributions require that only the stream name is
 signed.\n";
        print STDERR "The stream name is everything after, but not including, cfx/st/
\n";
        return 0;
    } else {
        return 1;
    }
}

# flash requires that the query parameters in the stream name are url
# encoded when passed in through javascript, etc.  This sub handles the minimal
# required url encoding.
sub escape_url_for_webpage {
    my ($url) = @_;

    $url =~ s/\?/%3F/g;
    $url =~ s/=/%3D/g;
    $url =~ s/&/%26/g;

    return $url;
}

1;
```

Créer une signature d’URL avec PHP

Tout serveur Web qui exécute PHP peut utiliser cet exemple de code PHP pour créer des déclarations de politique et des signatures pour CloudFront des distributions privées. L'exemple complet crée une page Web fonctionnelle avec des liens URL signés qui diffusent un flux vidéo via le CloudFront streaming. Vous pouvez télécharger l’exemple complet depuis le fichier demo-php.zip.

Remarques

- La création d'une signature d'URL n'est qu'une partie du processus d'offre d'un contenu privé avec une URL signée. Pour plus d'informations sur la totalité du processus, consultez Utilisation des URL signées.
- Vous pouvez aussi créer des URL signées à l'aide de la classe `UrlSigner` du AWS SDK pour PHP. Pour plus d'informations, consultez la section Classe UrlSigner dans la référence de AWS SDK pour PHP l'API.
- Dans l'`openssl_sign`appel, notez que passer `OPENSSL_ALGO_SHA256` en tant que quatrième argument passe à SHA-256. (Voir également le Création de cookies signés avec PHP pour un exemple complet.)

Rubriques

- Création de la signature RSA SHA-1
- Création d'une politique prédéfinie
- Créer une stratégie personnalisée
- Exemple de code complet

Les sections suivantes décomposent l'exemple de code en plusieurs parties. Vous trouverez le Exemple de code complet ci-dessous.

Création de la signature RSA SHA-1

Cet exemple de code effectue les opérations suivantes :

- La fonction `rsa_sha1_sign` hache et signe la déclaration de politique. Les arguments requis sont une déclaration de politique et la clé privée qui correspond à une clé publique qui se trouve dans un groupe de clés approuvé pour votre distribution.
- Ensuite, la `url_safe_base64_encode` fonction crée une URL-safe version de la signature.

```
function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";

    // load the private key
```

```
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);

    // compute signature
    openssl_sign($policy, $signature, $pkeyid);

    // free the key from memory
    openssl_free_key($pkeyid);

    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    // replace unsafe characters +, = and / with
    // the safe characters -, _ and ~
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}
```

L'extrait de code suivant utilise les fonctions `get_canned_policy_stream_name()` et permet de `get_custom_policy_stream_name()` créer une politique prédéfinie et personnalisée. CloudFront utilise les règles pour créer l'URL de diffusion de la vidéo, notamment en spécifiant la date d'expiration.

Vous pouvez ensuite utiliser une politique prédéfinie ou personnalisée pour définir la gestion de l’accès à votre contenu. Pour savoir quelle option privilégier, consultez la section Choix entre des politiques prédéfinies et personnalisées pour les URL signées.

Création d’une politique prédéfinie

L’exemple de code suivant construit une déclaration de politique prédéfinie pour la signature.

> **Note**
>
> La `$expires` variable est un date/time tampon qui doit être un entier et non une chaîne.

```
function get_canned_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $expires) {
    // this policy is well known by CloudFront, but you still need to sign it, since it
 contains your parameters
    $canned_policy = '{"Statement":[{"Resource":"' . $video_path . '","Condition":
{"DateLessThan":{"AWS:EpochTime":'. $expires . '}}}]}';
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($canned_policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // URL-encode the query string characters
    return $stream_name;
}
```

Pour plus d'informations sur les politiques prédéfinies, consultez Création d'une URL signée à l'aide d'une politique prédéfinie.

Créer une stratégie personnalisée

L'exemple de code suivant construit une déclaration de politique personnalisée pour la signature.

```
function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // URL-encode the query string characters
    return $stream_name;
```

```
}
```

Pour plus d'informations sur les politiques personnalisées, consultez Création d'une URL signée utilisant une politique personnalisée.

Exemple de code complet

L'exemple de code suivant fournit une démonstration complète de la création d'URL CloudFront signées avec PHP. Vous pouvez télécharger l'exemple complet depuis le fichier demo-php.zip.

Dans l'exemple suivant, vous pouvez modifier l'élément `$policy` `Condition` pour autoriser à la fois des plages d'adresses IPv4 et IPv6. Consultez par exemple Utilisation d'adresses IPv6 dans les politiques IAM dans le Guide de l'utilisateur Amazon Simple Storage Service.

```
<?php

function rsa_sha1_sign($policy, $private_key_filename) {
    $signature = "";

    // load the private key
    $fp = fopen($private_key_filename, "r");
    $priv_key = fread($fp, 8192);
    fclose($fp);
    $pkeyid = openssl_get_privatekey($priv_key);

    // compute signature
    openssl_sign($policy, $signature, $pkeyid);

    // free the key from memory
    openssl_free_key($pkeyid);

    return $signature;
}

function url_safe_base64_encode($value) {
    $encoded = base64_encode($value);
    // replace unsafe characters +, = and / with the safe characters -, _ and ~
    return str_replace(
        array('+', '=', '/'),
        array('-', '_', '~'),
        $encoded);
}
```

```
function create_stream_name($stream, $policy, $signature, $key_pair_id, $expires) {
    $result = $stream;
    // if the stream already contains query parameters, attach the new query parameters
 to the end
    // otherwise, add the query parameters
    $separator = strpos($stream, '?') == FALSE ? '?' : '&';
    // the presence of an expires time means we're using a canned policy
    if($expires) {
        $result .= $separator . "Expires=" . $expires . "&Signature=" . $signature .
 "&Key-Pair-Id=" . $key_pair_id;
    }
    // not using a canned policy, include the policy itself in the stream name
    else {
        $result .= $separator . "Policy=" . $policy . "&Signature=" . $signature .
 "&Key-Pair-Id=" . $key_pair_id;
    }

    // new lines would break us, so remove them
    return str_replace('\n', '', $result);
}


function get_canned_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $expires) {
    // this policy is well known by CloudFront, but you still need to sign it, since it
 contains your parameters
    $canned_policy = '{"Statement":[{"Resource":"' . $video_path . '","Condition":
{"DateLessThan":{"AWS:EpochTime":'. $expires . '}}}]}';
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($canned_policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($canned_policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, null, $encoded_signature,
 $key_pair_id, $expires);
    // URL-encode the query string characters
    return $stream_name;
}
```

```
function get_custom_policy_stream_name($video_path, $private_key_filename,
 $key_pair_id, $policy) {
    // the policy contains characters that cannot be part of a URL, so we base64 encode
 it
    $encoded_policy = url_safe_base64_encode($policy);
    // sign the original policy, not the encoded version
    $signature = rsa_sha1_sign($policy, $private_key_filename);
    // make the signature safe to be included in a URL
    $encoded_signature = url_safe_base64_encode($signature);

    // combine the above into a stream name
    $stream_name = create_stream_name($video_path, $encoded_policy, $encoded_signature,
 $key_pair_id, null);
    // URL-encode the query string characters
    return $stream_name;
}


// Path to your private key.  Be very careful that this file is not accessible
// from the web!

$private_key_filename = '/home/test/secure/example-priv-key.pem';
$key_pair_id = 'K2JCJMDEHXQW5F';

// Make sure you have "Restrict viewer access" enabled on this path behaviour and using
 the above Trusted key groups (recommended).
$video_path = 'https://example.com/secure/example.mp4';

$expires = time() + 300; // 5 min from now
$canned_policy_stream_name = get_canned_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $expires);

// Get the viewer real IP from the x-forward-for header as $_SERVER['REMOTE_ADDR']
 will return viewer facing IP. An alternative option is to use CloudFront-Viewer-
Address header. Note that this header is a trusted CloudFront immutable header. Example
 format: IP:PORT ("CloudFront-Viewer-Address": "1.2.3.4:12345")
$client_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
$policy =
'{'.
    '"Statement":['.
        '{'.
            '"Resource":"'. $video_path . '",'.
            '"Condition":{'.
                '"IpAddress":{"AWS:SourceIp":"' . $client_ip . '/32"},'.
```

```
                '"DateLessThan":{"AWS:EpochTime":' . $expires . '}'.
            '}'.
        '}'.
    ']' .
    '}';
$custom_policy_stream_name = get_custom_policy_stream_name($video_path,
 $private_key_filename, $key_pair_id, $policy);

?>

<html>

<head>
    <title>CloudFront</title>
</head>

<body>
    <h1>Amazon CloudFront</h1>
    <h2>Canned Policy</h2>
    <h3>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?></h3>
    <br />

    <div id='canned'>The canned policy video will be here: <br>

        <video width="640" height="360" autoplay muted controls>
        <source src="<?php echo $canned_policy_stream_name; ?>" type="video/mp4">
        Your browser does not support the video tag.
        </video>
    </div>

    <h2>Custom Policy</h2>
    <h3>Expires at <?php echo gmdate('Y-m-d H:i:s T', $expires); ?> only viewable by IP
 <?php echo $client_ip; ?></h3>
    <div id='custom'>The custom policy video will be here: <br>

         <video width="640" height="360" autoplay muted controls>
         <source src="<?php echo $custom_policy_stream_name; ?>" type="video/mp4">
         Your browser does not support the video tag.
        </video>
    </div>

</body>
```

```
</html>
```

Pour obtenir plus exemples sur la signature d'URL, consultez les rubriques suivantes :

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec C# et .NET Framework
- Créer une signature d'URL avec Java

Au lieu d'utiliser des URL signées pour créer la signature, vous pouvez utiliser des cookies signés. Pour plus d'informations, consultez Création de cookies signés avec PHP.

Créer une signature d'URL avec C# et .NET Framework

Les exemples C# de cette section implémentent un exemple d'application qui montre comment créer les signatures pour les distributions CloudFront privées à l'aide de déclarations de politique prédéfinies et personnalisées. Les exemples incluent des fonctions utilitaires basées sur le AWS SDK pour .NET pour .NET et qui peuvent être utiles dans les applications .NET.

Vous pouvez aussi créer des URL et des cookies signés à l'aide du SDK pour .NET. Dans la Référence des API du kit SDK pour .NET , consultez les rubriques suivantes :

- URL signées — AmazonCloudFrontUrlSigner
- Cookies signés — AmazonCloudFrontCookieSigner

Pour télécharger le code, consultez Code de signature en C#.

> **Remarques**
>
> - Les classes `AmazonCloudFrontUrlSigner` et `AmazonCloudFrontCookieSigner` ont été déplacées vers un package distinct. Pour plus d'informations sur leur utilisation, consultez CookieSigner et UrlSigner dans le Guide du développeur AWS SDK pour .NET (V4).
> - La création d'une signature d'URL n'est qu'une partie du processus d'offre d'un contenu privé avec une URL signée. Pour plus d'informations, consultez Utilisation des URL signées. Pour plus d'informations sur l'utilisation des cookies signés, consultez Utilisation de cookies signés.

- Dans l'appel de signature RSA, notez que cela SHA1 peut être remplacé par SHA256 dans le paramètre de l'algorithme de hachage.

Utilisation d’une clé RSA dans .NET Framework

Pour utiliser une clé RSA dans le .NET Framework, vous devez convertir le fichier .pem AWS fourni au format XML utilisé par le .NET Framework.

Après la conversion, le fichier de clé privée RSA est au format suivant :

Example: clé privée RSA au format XML .NET Framework

```
<RSAKeyValue>
  <Modulus>
    wO5IvYCP5UcoCKDo1dcspoMehWBZcyfs9QEzGi6Oe5y+ewGr1oW+vB2GPB
    ANBiVPcUHTFWhwaIBd3oglmF0lGQljP/jOfmXHUK2kUUnLnJp+oOBL2NiuFtqcW6h/L5lIpD8Yq+NRHg
    Ty4zDsyr2880MvXv88yEFURCkqEXAMPLE=
  </Modulus>
  <Exponent>AQAB</Exponent>
  <P>
    5bmKDaTz
    npENGVqz4Cea8XPH+sxt+2VaAwYnsarVUoSBeVt8WLloVuZGG9IZYmH5KteXEu7fZveYd9UEXAMPLE==
  </P>
  <Q>
    1v9l/WN1a1N3rOK4VGoCokx7kR2SyTMSbZgF9IWJNOugR/WZw7HTnjipO3c9dy1Ms9pUKwUF4
    6d7049EXAMPLE==
  </Q>
  <DP>
    RgrSKuLWXMyBH+/l1Dx/I4tXuAJIrlPyo+VmiOc7b5NzHptkSHEPfR9s1
    OK0VqjknclqCJ3Ig86OMEtEXAMPLE==
  </DP>
  <DQ>
    pjPjvSFw+RoaTu0pgCA/jwW/FGyfN6iim1RFbkT4
    z49DZb2IM885f3vf35eLTaEYRYUHQgZtChNEV0TEXAMPLE==
  </DQ>
  <InverseQ>
    nkvOJTg5QtGNgWb9i
    cVtzrL/1pFEOHbJXwEJdU99N+7sMK+1066DL/HSBUCD63qD4USpnf0myc24in0EXAMPLE==</InverseQ>
  <D>
      Bc7mp7XYHynuPZxChjWNJZIq+A73gm0ASDv6At7F8Vi9r0xUlQe/v0AQS3ycN8QlyR4XMbzMLYk
      3yjxFDXo4ZKQtOGzLGteCU2srANiLv26/imXA8FVidZftTAtLviWQZBVPTeYIA69ATUYPEq0a5u5wjGy
      UOij9OWyuEXAMPLE=
```

```
   </D>
</RSAKeyValue>
```

Méthode de signature de politique prédéfinie en C#

Le code C# suivant crée une URL signée qui utilise une politique prédéfinie en effectuant les opérations suivantes :

- Crée une déclaration de politique.
- Hache la déclaration de politique avec SHA1 et signe le résultat à l'aide de RSA et de la clé privée dont la clé publique correspondante se trouve dans un groupe de clés approuvé.
- Base64-encodes la déclaration de politique hachée et signée et remplace les caractères spéciaux pour que la chaîne puisse être utilisée en toute sécurité comme paramètre de demande d'URL.
- Concatène les valeurs.

Pour l'implémentation complète, consultez l'exemple de la rubrique Code de signature en C#.

> **Note**
>
> Le `keyId` est renvoyé lorsque vous téléchargez une clé publique sur CloudFront. Pour plus d'informations, consultez
>
> 6
>
> & Key-Pair-Id.

Example: méthode de signature de politique prédéfinie en C#

```
public static string ToUrlSafeBase64String(byte[] bytes)
{
    return System.Convert.ToBase64String(bytes)
        .Replace('+', '-')
        .Replace('=', '_')
        .Replace('/', '~');
}

public static string CreateCannedPrivateURL(string urlString,
    string durationUnits, string durationNumber, string pathToPolicyStmnt,
    string pathToPrivateKey, string keyId)
{
```

```
    // args[] 0-thisMethod, 1-resourceUrl, 2-seconds-minutes-hours-days
    // to expiration, 3-numberOfPreviousUnits, 4-pathToPolicyStmnt,
    // 5-pathToPrivateKey, 6-keyId

    TimeSpan timeSpanInterval = GetDuration(durationUnits, durationNumber);

    // Create the policy statement.
    string strPolicy = CreatePolicyStatement(pathToPolicyStmnt,
        urlString,
        DateTime.Now,
        DateTime.Now.Add(timeSpanInterval),
        "0.0.0.0/0");
    if ("Error!" == strPolicy) return "Invalid time frame." +
        "Start time cannot be greater than end time.";

    // Copy the expiration time defined by policy statement.
    string strExpiration = CopyExpirationTimeFromPolicy(strPolicy);

    // Read the policy into a byte buffer.
    byte[] bufferPolicy = Encoding.ASCII.GetBytes(strPolicy);

    // Initialize the SHA1CryptoServiceProvider object and hash the policy data.
    using (SHA1CryptoServiceProvider
        cryptoSHA1 = new SHA1CryptoServiceProvider())
    {
        bufferPolicy = cryptoSHA1.ComputeHash(bufferPolicy);

        // Initialize the RSACryptoServiceProvider object.
        RSACryptoServiceProvider providerRSA = new RSACryptoServiceProvider();
        XmlDocument xmlPrivateKey = new XmlDocument();

        // Load your private key, which you created by converting your
        // .pem file to the XML format that the .NET framework uses.
        // Several tools are available.
        xmlPrivateKey.Load(pathToPrivateKey);

        // Format the RSACryptoServiceProvider providerRSA and
        // create the signature.
        providerRSA.FromXmlString(xmlPrivateKey.InnerXml);
        RSAPKCS1SignatureFormatter rsaFormatter =
            new RSAPKCS1SignatureFormatter(providerRSA);
        rsaFormatter.SetHashAlgorithm("SHA1");
        byte[] signedPolicyHash = rsaFormatter.CreateSignature(bufferPolicy);
```

```
        // Convert the signed policy to URL-safe base64 encoding and
        // replace unsafe characters + = / with the safe characters - _ ~
        string strSignedPolicy = ToUrlSafeBase64String(signedPolicyHash);

        // Concatenate the URL, the timestamp, the signature,
        // and the key pair ID to form the signed URL.
        return urlString +
            "?Expires=" +
            strExpiration +
            "&Signature=" +
            strSignedPolicy +
            "&Key-Pair-Id=" +
            keyId;
    }
}
```

Méthode de signature de politique personnalisée en C#

Le code C# suivant crée une URL signée qui utilise une politique personnalisée en effectuant les opérations suivantes :

1. Crée une déclaration de politique.
2. Base64-encodes la déclaration de politique et remplace les caractères spéciaux pour que la chaîne puisse être utilisée en toute sécurité comme paramètre de demande d'URL.
3. Hache la déclaration de politique avec SHA1 et chiffre le résultat à l'aide de RSA et de la clé privée dont la clé publique correspondante se trouve dans un groupe de clés approuvé.
4. Base64-encodes la déclaration de politique hachée et le remplacement des caractères spéciaux pour que la chaîne puisse être utilisée en toute sécurité comme paramètre de demande d'URL.
5. Concatène les valeurs.

Pour l'implémentation complète, consultez l'exemple de la rubrique Code de signature en C#.

> **Note**
>
> Le `keyId` est renvoyé lorsque vous téléchargez une clé publique sur CloudFront. Pour plus d'informations, consultez
>
> 
>
> & Key-Pair-Id.

Example: méthode de signature de politique personnalisée en C#

```
public static string ToUrlSafeBase64String(byte[] bytes)
{
    return System.Convert.ToBase64String(bytes)
        .Replace('+', '-')
        .Replace('=', '_')
        .Replace('/', '~');
}

public static string CreateCustomPrivateURL(string urlString,
    string durationUnits, string durationNumber, string startIntervalFromNow,
    string ipaddress, string pathToPolicyStmnt, string pathToPrivateKey,
    string keyId)
{
    // args[] 0-thisMethod, 1-resourceUrl, 2-seconds-minutes-hours-days
    // to expiration, 3-numberOfPreviousUnits, 4-starttimeFromNow,
    // 5-ip_address, 6-pathToPolicyStmt, 7-pathToPrivateKey, 8-keyId

    TimeSpan timeSpanInterval = GetDuration(durationUnits, durationNumber);
    TimeSpan timeSpanToStart = GetDurationByUnits(durationUnits,
        startIntervalFromNow);
    if (null == timeSpanToStart)
        return "Invalid duration units." +
            "Valid options: seconds, minutes, hours, or days";

    string strPolicy = CreatePolicyStatement(
        pathToPolicyStmnt, urlString, DateTime.Now.Add(timeSpanToStart),
        DateTime.Now.Add(timeSpanInterval), ipaddress);

    // Read the policy into a byte buffer.
    byte[] bufferPolicy = Encoding.ASCII.GetBytes(strPolicy);

    // Convert the policy statement to URL-safe base64 encoding and
    // replace unsafe characters + = / with the safe characters - _ ~

    string urlSafePolicy = ToUrlSafeBase64String(bufferPolicy);

    // Initialize the SHA1CryptoServiceProvider object and hash the policy data.
    byte[] bufferPolicyHash;
    using (SHA1CryptoServiceProvider cryptoSHA1 =
        new SHA1CryptoServiceProvider())
    {
        bufferPolicyHash = cryptoSHA1.ComputeHash(bufferPolicy);
```

```
        // Initialize the RSACryptoServiceProvider object.
        RSACryptoServiceProvider providerRSA = new RSACryptoServiceProvider();
        XmlDocument xmlPrivateKey = new XmlDocument();

        // Load your private key, which you created by converting your
        // .pem file to the XML format that the .NET framework uses.
        // Several tools are available.
        xmlPrivateKey.Load(pathToPrivateKey);

        // Format the RSACryptoServiceProvider providerRSA
        // and create the signature.
        providerRSA.FromXmlString(xmlPrivateKey.InnerXml);
        RSAPKCS1SignatureFormatter RSAFormatter =
            new RSAPKCS1SignatureFormatter(providerRSA);
        RSAFormatter.SetHashAlgorithm("SHA1");
        byte[] signedHash = RSAFormatter.CreateSignature(bufferPolicyHash);

        // Convert the signed policy to URL-safe base64 encoding and
        // replace unsafe characters + = / with the safe characters - _ ~
        string strSignedPolicy = ToUrlSafeBase64String(signedHash);

        return urlString +
            "?Policy=" +
            urlSafePolicy +
            "&Signature=" +
            strSignedPolicy +
            "&Key-Pair-Id=" +
            keyId;
    }
}
```

Méthodes d’utilité pour la génération de signatures

Les méthodes suivantes obtiennent la déclaration de politique d’un fichier et analyse les intervalles de temps pour la génération des signatures.

Example: méthodes d’utilité pour la génération de signatures

```
public static string CreatePolicyStatement(string policyStmnt,
   string resourceUrl,
   DateTime startTime,
   DateTime endTime,
   string ipAddress)
```

```
{
   // Create the policy statement.
   FileStream streamPolicy = new FileStream(policyStmnt, FileMode.Open,
 FileAccess.Read);
   using (StreamReader reader = new StreamReader(streamPolicy))
   {
      string strPolicy = reader.ReadToEnd();

      TimeSpan startTimeSpanFromNow = (startTime - DateTime.Now);
      TimeSpan endTimeSpanFromNow = (endTime - DateTime.Now);
      TimeSpan intervalStart =
         (DateTime.UtcNow.Add(startTimeSpanFromNow)) -
         new DateTime(1970, 1, 1, 0, 0, 0, DateTimeKind.Utc);
      TimeSpan intervalEnd =
         (DateTime.UtcNow.Add(endTimeSpanFromNow)) -
         new DateTime(1970, 1, 1, 0, 0, 0, DateTimeKind.Utc);

      int startTimestamp = (int)intervalStart.TotalSeconds; // START_TIME
      int endTimestamp = (int)intervalEnd.TotalSeconds;  // END_TIME

      if (startTimestamp > endTimestamp)
         return "Error!";

      // Replace variables in the policy statement.
      strPolicy = strPolicy.Replace("RESOURCE", resourceUrl);
      strPolicy = strPolicy.Replace("START_TIME", startTimestamp.ToString());
      strPolicy = strPolicy.Replace("END_TIME", endTimestamp.ToString());
      strPolicy = strPolicy.Replace("IP_ADDRESS", ipAddress);
      strPolicy = strPolicy.Replace("EXPIRES", endTimestamp.ToString());
      return strPolicy;
   }
}

public static TimeSpan GetDuration(string units, string numUnits)
{
   TimeSpan timeSpanInterval = new TimeSpan();
   switch (units)
   {
      case "seconds":
         timeSpanInterval = new TimeSpan(0, 0, 0, int.Parse(numUnits));
         break;
      case "minutes":
         timeSpanInterval = new TimeSpan(0, 0, int.Parse(numUnits), 0);
```

```
         break;
      case "hours":
         timeSpanInterval = new TimeSpan(0, int.Parse(numUnits), 0 ,0);
         break;
      case "days":
         timeSpanInterval = new TimeSpan(int.Parse(numUnits),0 ,0 ,0);
         break;
      default:
         Console.WriteLine("Invalid time units;" +
            "use seconds, minutes, hours, or days");
         break;
   }
   return timeSpanInterval;
}

private static TimeSpan GetDurationByUnits(string durationUnits,
   string startIntervalFromNow)
{
   switch (durationUnits)
   {
      case "seconds":
         return new TimeSpan(0, 0, int.Parse(startIntervalFromNow));
      case "minutes":
         return new TimeSpan(0, int.Parse(startIntervalFromNow), 0);
      case "hours":
         return new TimeSpan(int.Parse(startIntervalFromNow), 0, 0);
      case "days":
         return new TimeSpan(int.Parse(startIntervalFromNow), 0, 0, 0);
      default:
         return new TimeSpan(0, 0, 0, 0);
   }
}

public static string CopyExpirationTimeFromPolicy(string policyStatement)
{
   int startExpiration = policyStatement.IndexOf("EpochTime");
   string strExpirationRough = policyStatement.Substring(startExpiration +
      "EpochTime".Length);
   char[] digits = { '0', '1', '2', '3', '4', '5', '6', '7', '8', '9' };

   List<char> listDigits = new List<char>(digits);
   StringBuilder buildExpiration = new StringBuilder(20);

   foreach (char c in strExpirationRough)
```

```
    {
        if (listDigits.Contains(c))
            buildExpiration.Append(c);
    }
    return buildExpiration.ToString();
}
```

Voir aussi

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec Java

Créer une signature d'URL avec Java

Outre l'exemple de code suivant, vous pouvez utiliser la classe `CloudFrontUrlSigner` utilitaire de la AWS SDK pour Java (version 1) pour créer des URL CloudFront signées.

Pour plus d'exemples, voir Création d'URL signées et de cookies à l'aide d'un AWS SDK dans la bibliothèque de codes d'exemples de code du AWS SDK.

> **Remarques**
>
> - La création d'une URL signée n'est qu'une partie du processus de diffusion de contenu privé avec CloudFront. Pour plus d'informations sur la totalité du processus, consultez Utilisation des URL signées.
> - Lors de l'`Signature.getInstance`appel, notez qu'il `SHA1withRSA` peut être remplacé par`SHA256withRSA`.

Example Méthodes de chiffrement de politiques et de signatures Java

```
package org.example;

import java.time.Instant;
import java.time.temporal.ChronoUnit;
import software.amazon.awssdk.services.cloudfront.CloudFrontUtilities;
import software.amazon.awssdk.services.cloudfront.model.CannedSignerRequest;
import software.amazon.awssdk.services.cloudfront.url.SignedUrl;
```

```
public class Main {

    public static void main(String[] args) throws Exception {
        CloudFrontUtilities cloudFrontUtilities = CloudFrontUtilities.create();
        Instant expirationDate = Instant.now().plus(7, ChronoUnit.DAYS);
        String resourceUrl = "https://a1b2c3d4e5f6g7.cloudfront.net";
        String keyPairId = "K1UA3WV15I7JSD";
        CannedSignerRequest cannedRequest = CannedSignerRequest.builder()
                .resourceUrl(resourceUrl)
                .privateKey(new java.io.File("/path/to/private_key.pem").toPath())
                .keyPairId(keyPairId)
                .expirationDate(expirationDate)
                .build();
        SignedUrl signedUrl =
 cloudFrontUtilities.getSignedUrlWithCannedPolicy(cannedRequest);
        String url = signedUrl.url();
        System.out.println(url);

    }
}
```

Example Exemple de signature de politique standardisée avec SHA256 en Java

```
package org.example;

import java.io.File;
import java.nio.file.Files;
import java.security.KeyFactory;
import java.security.PrivateKey;
import java.security.Signature;
import java.security.spec.PKCS8EncodedKeySpec;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.Base64;

public class Main {

    public static void main(String[] args) throws Exception {
        String resourceUrl = "https://a1b2c3d4e5f6g7.cloudfront.net/myfile.html";
        String keyPairId = "K1UA3WV15I7JSD";
        Instant expiration = Instant.now().plus(7, ChronoUnit.DAYS);
        PrivateKey privateKey = loadPrivateKey("/path/to/private_key.der");
```

```
        System.out.println(createSignedUrl(resourceUrl, keyPairId, privateKey,
expiration, "SHA1"));
        System.out.println(createSignedUrl(resourceUrl, keyPairId, privateKey,
expiration, "SHA256"));
    }

    static String createSignedUrl(String resourceUrl, String keyPairId,
                                  PrivateKey privateKey, Instant expiration,
                                  String hashAlgorithm) throws Exception {
        long epochSeconds = expiration.getEpochSecond();

        String policy = "{\"Statement\":[{\"Resource\":\"" + resourceUrl
                + "\",\"Condition\":{\"DateLessThan\":{\"AWS:EpochTime\":" +
epochSeconds + "}}}]}";

        String jcaAlgorithm = hashAlgorithm.equals("SHA256") ? "SHA256withRSA" :
"SHA1withRSA";

        Signature sig = Signature.getInstance(jcaAlgorithm);
        sig.initSign(privateKey);
        sig.update(policy.getBytes("UTF-8"));
        String signature = base64UrlEncode(sig.sign());

        String url = resourceUrl
                + (resourceUrl.contains("?") ? "&" : "?")
                + "Expires=" + epochSeconds
                + "&Signature=" + signature
                + "&Key-Pair-Id=" + keyPairId;

        if (hashAlgorithm.equals("SHA256")) {
            url += "&Hash-Algorithm=SHA256";
        }

        return url;
    }

    static String base64UrlEncode(byte[] bytes) {
        return Base64.getEncoder().encodeToString(bytes)
                .replace('+', '-')
                .replace('=', '_')
                .replace('/', '~');
    }
```

```
    static PrivateKey loadPrivateKey(String path) throws Exception {
        byte[] keyBytes = Files.readAllBytes(new File(path).toPath());
        return KeyFactory.getInstance("RSA")
                .generatePrivate(new PKCS8EncodedKeySpec(keyBytes));
    }
}
```

Voir aussi :

- Créer une signature d'URL avec Perl
- Créer une signature d'URL avec PHP
- Créer une signature d'URL avec C# et .NET Framework

Restreindre l'accès à un AWS origine

Vous pouvez configurer CloudFront certaines AWS origines d'une manière qui offre les avantages suivants :

- Restreint l'accès à l' AWS origine afin qu'elle ne soit pas accessible au public.
- Veille à ce que les spectateurs (utilisateurs) puissent accéder au contenu de l' AWS origine uniquement par le biais de la CloudFront distribution spécifiée. Cela empêche les spectateurs d'accéder au contenu directement depuis l'origine ou par le biais d'une CloudFront distribution involontaire.

Pour ce faire, configurez CloudFront pour envoyer des demandes authentifiées à votre AWS origine, et configurez l' AWS origine pour autoriser uniquement l'accès aux demandes authentifiées provenant de. CloudFront Pour plus d'informations, consultez les rubriques suivantes pour connaître les types d' AWS origines compatibles.

Rubriques

- Restreindre l'accès à une origine AWS Elemental MediaPackage v2
- Restreindre l'accès à un AWS Elemental MediaStore origine
- Restreindre l'accès à un AWS Lambda origine de l'URL de la fonction
- Restreindre l'accès à un AWS Lambda Origine de la fonction Web
- Restriction de l'accès à une origine Amazon S3
- Restriction de l'accès avec les origines de VPC

- Restreindre l'accès à l'origine d'un point Multi-Region d'accès Amazon S3

Restreindre l'accès à une origine AWS Elemental MediaPackage v2

CloudFront fournit un contrôle d'accès à l'origine (OAC) pour restreindre l'accès à une origine MediaPackage v2.

> **Note**
>
> CloudFront OAC ne prend en charge que la MediaPackage v2. MediaPackage la v1 n'est pas prise en charge.

Rubriques

- Création d’un nouvel OAC
- Paramètres avancés pour le contrôle d’accès à l’origine

Création d’un nouvel OAC

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouvel OAC dans CloudFront.

Rubriques

- Conditions préalables
- Accorder CloudFront l'autorisation d'accéder à l'origine de la MediaPackage version 2
- Création de l’OAC

Conditions préalables

Avant de créer et de configurer OAC, vous devez disposer d'une CloudFront distribution d'origine MediaPackage v2. Pour de plus amples informations, veuillez consulter Utiliser un MediaStore conteneur ou un MediaPackage canal.

Accorder CloudFront l'autorisation d'accéder à l'origine de la MediaPackage version 2

Avant de créer un OAC ou de le configurer dans une CloudFront distribution, assurez-vous qu'il CloudFront est autorisé à accéder à l'origine MediaPackage v2. Procédez ainsi après avoir créé une

CloudFront distribution, mais avant d'ajouter l'OAC à l'origine MediaPackage v2 dans la configuration de distribution.

Utilisez une politique IAM pour autoriser le principal de CloudFront service (`cloudfront.amazonaws.com`) à accéder à l'origine. L'`Condition`élément de la politique permet d'accéder CloudFront à l'origine MediaPackage v2 uniquement lorsque la demande est au nom de la CloudFront distribution qui contient l'origine MediaPackage v2. Il s'agit de la distribution avec l'origine MediaPackage v2 à laquelle vous souhaitez ajouter OAC.

Example: politique IAM qui autorise l'accès en lecture seule pour une CloudFront distribution avec OAC activé

La politique suivante autorise la CloudFront distribution (*E1PDK09ESKHJWT*) à accéder à l'origine MediaPackage v2. L'origine est l'ARN spécifié pour l'élément `Resource`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {"Service": "cloudfront.amazonaws.com"},
            "Action": "mediapackagev2:GetObject",
            "Resource": "arn:aws:mediapackagev2:us-
east-1:123456789012:channelGroup/channel-group-name/channel/channel-name/
originEndpoint/origin_endpoint_name",
            "Condition": {
                "StringEquals": {"AWS:SourceArn":
 "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT"}
            }
        }
    ]
}
```

Remarques

- Si vous avez activé la fonctionnalité MQAR et le contrôle d'accès d'origine (OAC), ajoutez l'action `mediapackagev2:GetHeadObject` à la politique IAM. MQAR a besoin de cette autorisation pour envoyer `HEAD` des demandes à l'origine MediaPackage v2. Pour plus d'informations sur MQAR, consultez Résilience tenant compte de la qualité média.
- Si vous créez une distribution qui n'est pas autorisée à accéder à votre origine MediaPackage v2, vous pouvez choisir Copier la politique depuis la CloudFront console, puis choisir Mettre à jour les autorisations du point de terminaison. Vous pouvez ensuite associer l'autorisation copiée au point de terminaison. Pour plus d'informations, consultez Champs de la politique de points de terminaison dans le Guide de l'utilisateur AWS Elemental MediaPackage .

Création de l'OAC

Pour créer un OAC, vous pouvez utiliser le Console de gestion AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un OAC

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur la page Créer un nouvel OAC, procédez comme suit :
   a. Entrez un Nom et éventuellement une Description pour l'OAC.
   b. Dans Comportement de signature, nous vous recommandons de conserver le paramètre par défaut Demandes de signature (recommandé). Pour de plus amples informations, veuillez consulter the section called "Paramètres avancés pour le contrôle d'accès à l'origine".
5. Pour le type d'origine, choisissez MediaPackage V2.
6. Choisissez Créer.

> **Tip**
>
> Après avoir créé l'OAC, prenez note du Nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un OAC à une origine MediaPackage v2 dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution d'origine MediaPackage V2 à laquelle vous souhaitez ajouter l'OAC, puis choisissez l'onglet Origins.
3. Sélectionnez l'origine MediaPackage v2 à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Sélectionnez HTTPS only (HTTPS uniquement) pour le paramètre Protocol (Protocole) de votre origine.
5. Dans le menu déroulant Contrôle d'accès d'origine, choisissez le nom de l'OAC que vous souhaitez utiliser.
6. Sélectionnez Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine MediaPackage v2.

CloudFormation

Pour créer un OAC avec CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du CloudFormation modèle, au format YAML, pour créer un OAC.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: mediapackagev2
      SigningBehavior: always
```

```
      SigningProtocol: sigv4
```

Pour plus d'informations, consultez la section AWS::CloudFront::OriginAccessContrôle dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

   ```
   aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
    origin-access-control.yaml
   ```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

   ```
   aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
   access-control.yaml
   ```

   Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à une origine MediaPackage v2 dans une CloudFront distribution.

Pour attacher un OAC à une origine MediaPackage v2 dans une distribution existante (CLI avec fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit avoir une origine MediaPackage v2.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
   - Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine MediaPackage v2.

API

Pour créer un OAC avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou un autre client d'API.

Après avoir créé un OAC, vous pouvez l'associer à une origine MediaPackage v2 dans une distribution, à l'aide de l'un des appels d'API suivants :

- Pour le rattacher à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'OAC dans le champ `OriginAccessControlId`, à l'intérieur d'une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence de tous les paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Paramètres avancés pour le contrôle d'accès à l'origine

La fonctionnalité CloudFront OAC inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

L'OAC contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d'utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l'API, la CLI et CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes qu'il envoie à l'origine de la MediaPackage v2.

Ne jamais signer les demandes d'origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l'API, la CLI et CloudFormation. Utilisez ce paramètre pour désactiver l'OAC pour toutes les origines dans l'ensemble des distributions qui utilisent cet OAC. Cela permet d'économiser du temps et des efforts par rapport à la suppression d'un OAC de toutes les origines et distributions qui l'utilisent, une par une. Avec ce paramètre, CloudFront ne signe aucune demande envoyée à l'origine de la MediaPackage v2.

> **Warning**
>
> Pour utiliser ce paramètre, l'origine MediaPackage v2 doit être accessible au public. Si vous utilisez ce paramètre avec une origine MediaPackage v2 qui n'est pas accessible au public, CloudFront vous ne pouvez pas accéder à l'origine. L'origine MediaPackage v2 renvoie les erreurs CloudFront et les CloudFront transmet aux spectateurs. Pour plus d'informations, consultez l'exemple de politique MediaPackage v2 pour les politiques et les autorisations MediaPackage dans le guide de AWS Elemental MediaPackage l'utilisateur.

Ne remplacez pas l'en-tête **`Authorization`** de l'utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et CloudFormation. Utilisez ce paramètre lorsque vous CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> **Warning**
>
> Pour transmettre l'`Authorization`en-tête de la demande du lecteur, vous devez l'`Authorization`ajouter à une politique de cache pour tous les comportements de cache qui utilisent des origines MediaPackage v2 associées à ce contrôle d'accès à l'origine.

Restreindre l'accès à un AWS Elemental MediaStore origine

CloudFront fournit un contrôle d'accès à l'origine (OAC) pour restreindre l'accès à une AWS Elemental MediaStore origine.

Rubriques

- Création d'un nouveau contrôle d'accès d'origine
- Paramètres avancés pour le contrôle d'accès à l'origine

Création d’un nouveau contrôle d’accès d’origine

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouveau contrôle d'accès à l'origine dans CloudFront.

Rubriques

- Conditions préalables
- Accorder CloudFront l'autorisation d'accéder à l' MediaStore origine
- Création du contrôle d’accès d’origine

Conditions préalables

Avant de créer et de configurer le contrôle d'accès à l'origine, vous devez disposer d'une CloudFront distribution avec une MediaStore origine.

Accorder CloudFront l'autorisation d'accéder à l' MediaStore origine

Avant de créer un contrôle d'accès à l'origine ou de le configurer dans une CloudFront distribution, assurez-vous que celui-ci CloudFront est autorisé à accéder à l' MediaStore origine. Procédez ainsi après avoir créé une CloudFront distribution, mais avant d'ajouter l'OAC à l' MediaStoreorigine dans la configuration de distribution.

Utilisez une politique de MediaStore conteneur pour autoriser le principal CloudFront de service (`cloudfront.amazonaws.com`) à accéder à l'origine. Utilisez un `Condition` élément de la politique pour autoriser l'accès CloudFront au MediaStore conteneur uniquement lorsque la demande est présentée au nom de la CloudFront distribution qui contient l' MediaStore origine. Il s'agit de la distribution avec l' MediaStore origine à laquelle vous souhaitez ajouter OAC.

Voici des exemples de politiques de MediaStore conteneur qui permettent à une CloudFront distribution d'accéder à une MediaStore origine.

Example MediaStore politique de conteneur qui autorise l'accès en lecture seule pour une CloudFront distribution avec OAC activé

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
```

```
            {
                "Sid": "AllowCloudFrontServicePrincipalReadOnly",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject"
                ],
                "Resource": "arn:aws:mediastore:us-
east-1:111122223333:container/<container name>/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

Example MediaStore politique de conteneur qui autorise l'accès en lecture et en écriture pour une CloudFront distribution avec OAC activé

JSON

```
{
        "Version":"2012-10-17",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipalReadWrite",
                "Effect": "Allow",
                "Principal": {
                  "Service": "cloudfront.amazonaws.com"
                },
                "Action": [
                  "mediastore:GetObject",
                  "mediastore:PutObject"
```

```
                ],
                "Resource": "arn:aws:mediastore:us-
east-1:111122223333:container/container-name/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
                    },
                    "Bool": {
                      "aws:SecureTransport": "true"
                    }
                }
            }
        ]
}
```

> **Note**
>
> Pour autoriser l'accès en écriture, vous devez configurer les méthodes HTTP autorisées à inclure PUT dans les paramètres de comportement de votre CloudFront distribution.

Création du contrôle d’accès d’origine

Pour créer un OAC, vous pouvez utiliser le Console de gestion AWS CloudFormation, AWS CLI, ou l' CloudFrontAPI.

Console

Pour créer un contrôle d’accès à l’origine

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur l'écran Créer un paramètre de contrôle, procédez comme suit :
   a. Dans le volet Détails, entrez un Nom et (éventuellement) une Description pour le contrôle d'accès à l'origine.

b. Dans le volet Paramètres, nous vous recommandons de conserver le paramètre par défaut (Signer les demandes (recommandé)). Pour plus d'informations, consultez the section called "Paramètres avancés pour le contrôle d'accès à l'origine".

5. MediaStore Choisissez dans le menu déroulant Type d'origine.
6. Cliquez sur Créer.

   Après avoir créé l'OAC, prenez note de Nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un contrôle d'accès à l'origine à une MediaStore origine dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution avec une MediaStore origine à laquelle vous souhaitez ajouter l'OAC, puis cliquez sur l'onglet Origines.
3. Sélectionnez l' MediaStore origine à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Sélectionnez HTTPS only (HTTPS uniquement) pour le paramètre Protocol (Protocole) de votre origine.
5. Dans le menu déroulant Origin access control (Contrôle d'accès d'origine), choisissez l'OAC que vous souhaitez utiliser.
6. Cliquez sur Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine du MediaStore compartiment.

CloudFormation

Pour créer un contrôle d'accès à l'origine (OAC) avec CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du CloudFormation modèle, au format YAML, pour créer un contrôle d'accès à l'origine.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
```

```
    Name: ExampleOAC
    OriginAccessControlOriginType: mediastore
    SigningBehavior: always
    SigningProtocol: sigv4
```

Pour plus d'informations, voir AWS::CloudFront: : OriginAccessControl dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

   ```
   aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
    origin-access-control.yaml
   ```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

   ```
   aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
   access-control.yaml
   ```

   Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à une MediaStore origine dans une CloudFront distribution.

Pour attacher un OAC à une MediaStore origine dans une distribution existante (CLI avec fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit avoir une MediaStore origine.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
   - Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l' MediaStore origine.

API

Pour créer un contrôle d'accès à l'origine avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé un contrôle d'accès à l'origine, vous pouvez l'associer à une MediaStore origine dans une distribution à l'aide de l'un des appels d'API suivants :

- Pour l'associer à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de contrôle d'accès à l'origine dans le champ `OriginAccessControlId`, à l'intérieur d'une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence de tous les paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Paramètres avancés pour le contrôle d’accès à l’origine

La fonctionnalité de contrôle CloudFront d'accès à l'origine inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

Le contrôle d'accès à Origin contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d’utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l’API, la CLI et CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes qu'il envoie à l' MediaStore origine.

Ne jamais signer les demandes d’origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l'API, la CLI et CloudFormation. Utilisez ce paramètre pour désactiver le contrôle d'accès à l'origine pour toutes les origines dans toutes les distributions qui utilisent ce contrôle d'accès à l'origine. Cela permet d’économiser du temps et des efforts par rapport à la suppression d’un contrôle d’accès à l’origine de toutes les origines et distributions qui l’utilisent, une par une. Avec ce paramètre, CloudFront ne signe aucune demande envoyée à l' MediaStoreorigine.

> **Warning**
>
> Pour utiliser ce paramètre, l' MediaStore origine doit être accessible au public. Si vous utilisez ce paramètre avec une MediaStore origine qui n'est pas accessible au public, vous CloudFront ne pouvez pas accéder à l'origine. L' MediaStore origine renvoie les erreurs CloudFront et les CloudFront transmet aux spectateurs. Pour plus d'informations, consultez l'exemple de politique de MediaStore conteneur pour l'accès public en lecture via HTTPS.

Ne remplacez pas l'en-tête **`Authorization`** de l'utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et CloudFormation. Utilisez ce paramètre lorsque vous CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> **Warning**
>
> Pour transmettre l'`Authorization`en-tête de la demande du lecteur, vous devez l'`Authorization`ajouter à une politique de cache pour tous les comportements de cache qui utilisent des MediaStore origines associées à ce contrôle d'accès aux origines.

Restreindre l'accès à un AWS Lambda origine de l'URL de la fonction

CloudFront fournit un contrôle d'accès à l'origine (OAC) pour restreindre l'accès à l'origine de l'URL d'une fonction Lambda.

> **Note**
>
> Si vous utilisez une fonction Web Lambda comme CloudFront origine, consultez. Restreindre l'accès à un AWS Lambda Origine de la fonction Web Les origines des fonctions Web Lambda nécessitent une configuration OAC différente.

Rubriques

- Création d’un nouvel OAC
- Paramètres avancés pour le contrôle d’accès à l’origine
- Exemple de code de modèle

Création d’un nouvel OAC

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouvel OAC dans CloudFront.

> **Important**
>
> Si vous utilisez `POST` des méthodes `PUT` or avec l'URL de votre fonction Lambda, vos utilisateurs doivent calculer le SHA256 du corps et inclure la valeur de hachage de la charge utile du corps de la demande dans l'`x-amz-content-sha256`en-tête lorsqu'ils envoient la demande à. CloudFront Lambda ne prend pas en charge les données utiles non signées.

Rubriques

- Conditions préalables
- CloudFront Autoriser l'accès à l'URL de la fonction Lambda
- Création de l’OAC

Conditions préalables

Avant de créer et de configurer OAC, vous devez disposer d'une CloudFront distribution avec une URL de fonction Lambda comme origine. Pour utiliser l’OAC, vous devez spécifier la valeur `AWS_IAM` pour le paramètre `AuthType`. Pour plus d’informations, consultez Utilisation d’une URL de fonction Lambda.

CloudFront Autoriser l'accès à l'URL de la fonction Lambda

Avant de créer un OAC ou de le configurer dans une CloudFront distribution, assurez-vous qu'il CloudFront est autorisé à accéder à l'URL de la fonction Lambda. Procédez ainsi après avoir créé une CloudFront distribution, mais avant d'ajouter l'OAC à l'URL de la fonction Lambda dans la configuration de distribution.

> **Note**
>
> Pour mettre à jour la politique IAM de l'URL de la fonction Lambda, vous devez utiliser l' AWS Command Line Interface (AWS CLI). La modification de la politique IAM dans la console Lambda n'est pas prise en charge pour le moment.

La AWS CLI commande suivante accorde au CloudFront service principal (`cloudfront.amazonaws.com`) l'accès à l'URL de votre fonction Lambda. L'`Condition`élément de la politique permet d'accéder CloudFront à Lambda uniquement lorsque la demande provient de la CloudFront distribution qui contient l'URL de la fonction Lambda. Il s'agit de la distribution contenant l'URL de la fonction Lambda à laquelle vous souhaitez ajouter l'OAC.

Example: AWS CLI commande pour mettre à jour une politique afin d'autoriser l'accès en lecture seule pour une CloudFront distribution avec OAC activé

Les AWS CLI commandes suivantes permettent à la CloudFront distribution (*E1PDK09ESKHJWT*) d'accéder à votre Lambda*FUNCTION_URL_NAME*.

```
aws lambda add-permission \
--statement-id "AllowCloudFrontServicePrincipal" \
--action "lambda:InvokeFunctionUrl" \
--principal "cloudfront.amazonaws.com" \
--source-arn "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT" \
--function-name FUNCTION_URL_NAME
```

```
aws lambda add-permission \
--statement-id "AllowCloudFrontServicePrincipalInvokeFunction" \
--action "lambda:InvokeFunction" \
--principal "cloudfront.amazonaws.com" \
--source-arn "arn:aws:cloudfront::123456789012:distribution/E1PDK09ESKHJWT" \
--function-name FUNCTION_URL_NAME
```

> **Note**
>
> Si vous créez une distribution et qu'elle n'est pas autorisée à accéder à l'URL de votre fonction Lambda, vous pouvez choisir la commande Copy CLI depuis la CloudFront console, puis entrer cette commande depuis votre terminal de ligne de commande. Pour plus

d'informations, consultez Attribution de l'accès à la fonction aux Services AWS dans le Guide du développeur AWS Lambda .

Création de l'OAC

Pour créer un OAC, vous pouvez utiliser le Console de gestion AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un OAC

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur la page Créer un nouvel OAC, procédez comme suit :
   a. Entrez un Nom et éventuellement une Description pour l'OAC.
   b. Dans Comportement de signature, nous vous recommandons de conserver le paramètre par défaut Demandes de signature (recommandé). Pour plus d'informations, consultez the section called "Paramètres avancés pour le contrôle d'accès à l'origine".
5. Pour Type de l'origine, choisissez Lambda.
6. Cliquez sur Créer.

> **Tip**
>
> Après avoir créé l'OAC, prenez note du Nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un contrôle d'accès d'origine à une URL de fonction Lambda dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution qui comporte l'URL de fonction Lambda à laquelle vous souhaitez ajouter l'OAC, puis choisissez l'onglet Origines.

3. Sélectionnez l'URL de fonction Lambda à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Sélectionnez HTTPS only (HTTPS uniquement) pour le paramètre Protocol (Protocole) de votre origine.
5. Dans le menu déroulant Contrôle d'accès d'origine, choisissez le nom de l'OAC que vous souhaitez utiliser.
6. Cliquez sur Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'URL de fonction Lambda.

CloudFormation

Pour créer un OAC avec CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du CloudFormation modèle, au format YAML, pour créer un OAC.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: lambda
      SigningBehavior: always
      SigningProtocol: sigv4
```

Pour plus d'informations, voir AWS::CloudFront: : OriginAccessControl dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d’accès à l’origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à l'URL d'une fonction Lambda dans CloudFront une distribution.

Pour attacher un OAC à une URL de fonction Lambda dans une distribution existante (CLI avec un fichier d’entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit disposer d’une URL de fonction Lambda comme origine.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

- Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
- Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'URL de fonction Lambda.

API

Pour créer un OAC avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou un autre client d'API.

Après avoir créé un OAC, vous pouvez l'attacher à une URL de fonction Lambda dans une distribution à l'aide de l'un des appels d'API suivants :

- Pour le rattacher à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'OAC dans le champ `OriginAccessControlId`, à l'intérieur d'une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Paramètres avancés pour le contrôle d’accès à l’origine

La fonctionnalité CloudFront OAC inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

L'OAC contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d’utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l’API, la CLI et CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes envoyées à l'URL de la fonction Lambda.

Ne jamais signer les demandes d’origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l’API, la CLI et CloudFormation. Utilisez ce paramètre pour désactiver l’OAC pour toutes les origines dans l’ensemble des distributions qui utilisent cet OAC. Cela permet d’économiser du temps et des efforts par rapport à la suppression d’un OAC de toutes les origines et distributions qui l’utilisent, une par une. Avec ce paramètre, CloudFront ne signe aucune demande envoyée à l'URL de la fonction Lambda.

> **Warning**
>
> Pour utiliser ce paramètre, l’URL de fonction Lambda doit être accessible au public. Si vous utilisez ce paramètre avec une URL de fonction Lambda qui n'est pas accessible au public, CloudFront vous ne pouvez pas accéder à l'origine. L'URL de la fonction Lambda renvoie des erreurs CloudFront et les CloudFront transmet aux utilisateurs. Pour plus d’informations, consultez Modèle de sécurité et d’authentification pour les URL de fonctions Lambda dans le Guide de l’utilisateur AWS Lambda .

Ne remplacez pas l’en-tête **`Authorization`** de l’utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et CloudFormation. Utilisez ce paramètre lorsque vous

CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> ⚠ Warning
>
> - Si vous utilisez ce paramètre, vous devez spécifier la signature Signature Version 4 pour l'URL de la fonction Lambda au lieu du nom ou du CloudFront CNAME de votre distribution. Lorsque l' CloudFront `Authorization`en-tête de la demande du visualiseur est transféré à l'URL de la fonction Lambda, Lambda valide la signature par rapport à l'hôte du domaine URL Lambda. Si la signature n'est pas basée sur le domaine de l'URL Lambda, l'hôte figurant dans la signature ne correspondra pas à celui utilisé par l'origine de l'URL Lambda. Ainsi, la demande échouera, entraînant une erreur de validation de signature.
> - Pour transmettre l'en-tête `Authorization` de la demande de l'utilisateur, vous devez ajouter l'en-tête `Authorization` à une politique de cache pour tous les comportements de cache qui utilisent les URL de fonction Lambda associées à ce contrôle d'accès d'origine.

Exemple de code de modèle

Si votre CloudFront origine est une URL de fonction Lambda associée à un OAC, vous pouvez utiliser le script Python suivant pour télécharger des fichiers vers la fonction Lambda avec la méthode. `POST`

Ce code suppose que vous avez configuré l'OAC avec le comportement de signature par défaut défini sur Toujours signer les demandes d'origine et que vous n'avez pas sélectionné le paramètre Ne pas remplacer l'en-tête d'autorisation.

Cette configuration permet à l'OAC de gérer correctement l'autorisation SigV4 avec Lambda à l'aide du nom d'hôte Lambda. Les données utiles sont signées à l'aide de SigV4 à partir de l'identité IAM autorisée pour l'URL de la fonction Lambda, laquelle est désignée comme type `IAM_AUTH`.

Le modèle montre comment gérer les valeurs de hachage des données utiles signées dans l'en-tête x-amz-content-sha256 pour les demandes `POST` provenant du côté client. Plus précisément, ce modèle est conçu pour gérer les données utiles des données de formulaire. Le modèle permet le

téléchargement sécurisé de fichiers vers l'URL CloudFront d'une fonction Lambda et AWS utilise des mécanismes d'authentification pour s'assurer que seules les demandes autorisées peuvent accéder à la fonction Lambda.

Le code inclut les fonctionnalités suivantes :

- Satisfait à l'exigence d'inclure le hachage des données utiles dans l'en-tête x-amz-content-sha256
- Utilise l'authentification SigV4 pour un accès sécurisé Service AWS
- Prend en charge les envois de fichiers à l'aide de données de formulaire en plusieurs parties
- Inclut la gestion des erreurs pour les exceptions de demande

```
import boto3
from botocore.auth import SigV4Auth
from botocore.awsrequest import AWSRequest
import requests
import hashlib
import os


def calculate_body_hash(body):
    return hashlib.sha256(body).hexdigest()


def sign_request(request, credentials, region, service):
    sigv4 = SigV4Auth(credentials, service, region)
    sigv4.add_auth(request)


def upload_file_to_lambda(cloudfront_url, file_path, region):
    # AWS credentials
    session = boto3.Session()
    credentials = session.get_credentials()

    # Prepare the multipart form-data
    boundary = "----------------------boundary"

    # Read file content
```

```
    with open(file_path, 'rb') as file:
        file_content = file.read()

    # Get the filename from the path
    filename = os.path.basename(file_path)

    # Prepare the multipart body
    body = (
        f'--{boundary}\r\n'
        f'Content-Disposition: form-data; name="file"; filename="{filename}"\r\n'
        f'Content-Type: application/octet-stream\r\n\r\n'
    ).encode('utf-8')
    body += file_content
    body += f'\r\n--{boundary}--\r\n'.encode('utf-8')

    # Calculate SHA256 hash of the entire body
    body_hash = calculate_body_hash(body)

    # Prepare headers
    headers = {
        'Content-Type': f'multipart/form-data; boundary={boundary}',
        'x-amz-content-sha256': body_hash
    }

    # Create the request
    request = AWSRequest(
        method='POST',
        url=cloudfront_url,
        data=body,
        headers=headers
    )

    # Sign the request
    sign_request(request, credentials, region, 'lambda')

    # Get the signed headers
    signed_headers = dict(request.headers)

    # Print request headers before sending
    print("Request Headers:")
    for header, value in signed_headers.items():
        print(f"{header}: {value}")

    try:
```

```
        # Send POST request with signed headers
        response = requests.post(
            cloudfront_url,
            data=body,
            headers=signed_headers
        )

        # Print response status and content
        print(f"\nStatus code: {response.status_code}")
        print("Response:", response.text)

        # Print response headers
        print("\nResponse Headers:")
        for header, value in response.headers.items():
            print(f"{header}: {value}")

    except requests.exceptions.RequestException as e:
        print(f"An error occurred: {e}")


# Usage
cloudfront_url = "https://d111111abcdef8.cloudfront.net"
file_path = r"filepath"
region = "us-east-1"  # example: "us-west-2"

upload_file_to_lambda(cloudfront_url, file_path, region)
```

Restreindre l'accès à un AWS Lambda Origine de la fonction Web

Vous pouvez utiliser le contrôle d'accès à l'origine (OAC) pour restreindre l'accès à l'origine d'une fonction AWS Lambda Web. Une fonction Web Lambda fournit son propre point de terminaison HTTPS régional ou mondial, que vous utilisez comme domaine d'origine pour votre CloudFront distribution. Pour plus d'informations sur les fonctions Web Lambda, consultez la section Fonctions AWS Lambda Web du manuel du AWS Lambda développeur.

> **Note**
>
> L'OAC avec Lambda Web Functions n'est pas pris en charge pour les points de terminaison globaux qui incluent des régions optionnelles. Si le point de terminaison achemine une demande vers une région optionnelle, il CloudFront ne peut pas signer la demande pour cette

région. L'origine renvoie alors une erreur HTTP 403 (Interdit). Toutes les régions associées au point de terminaison global doivent être des régions activées par défaut.

Pour plus d'informations sur l'utilisation d'OAC avec l'origine de l'URL d'une fonction Lambda, consultez. Restreindre l'accès à un AWS Lambda origine de l'URL de la fonction

Conditions préalables

Avant de créer et de configurer OAC, vous devez disposer d'une CloudFront distribution dont l'origine est une fonction Web Lambda. Le nom de domaine d'origine est le nom d'hôte du point de terminaison de la fonction Web Lambda. CloudFront identifie le type de point de terminaison à partir du nom d'hôte :

- Point de terminaison régional (`HomeRegion`et types de `PerRegion` points de terminaison) : le nom d'hôte se termine par `.lambda-web.`*`AWS-Region`*`.on.aws`
- Point de terminaison global (type de `MultiRegion` point de terminaison) : le nom d'hôte se termine par `.lambda-web.global.on.aws`

Votre configuration doit également répondre aux exigences suivantes :

- Type d'authentification du point de terminaison : le type d'authentification du point de terminaison doit être. `IamAuth` Avec`IamAuth`, le point de terminaison utilise Gestion des identités et des accès AWS (IAM) pour authentifier et autoriser les demandes. Pour les demandes provenant de CloudFront, l'autorisation est basée sur la politique basée sur les ressources de la fonction Web Lambda. CloudFront signe les demandes au nom du spectateur, et le point de terminaison valide la signature. Pour plus d'informations, consultez la section sur CloudFront l'intégration dans le guide du AWS Lambda développeur.
- Politique de cache — Si votre fonction Web Lambda utilise l'`Authorization`en-tête du visualiseur, vous devez ajouter l'en-tête à la politique de cache. Cette exigence s'applique à tous les comportements de cache qui utilisent l'origine. Pour les `HEAD` demandes `GET` et, CloudFront supprime l'`Authorization`en-tête avant de transférer la demande, sauf si l'en-tête figure dans la politique de cache. Pour plus d'informations, consultez En-têtes et CloudFront comportement des requêtes HTTP (origines personnalisées et Amazon S3).
- Politique de demande d'origine : utilisez une politique de demande d'origine qui exclut l'`Host`en-tête du téléspectateur. Les points de terminaison Lambda Web Function s'attendent à ce que l'`Host`en-tête contienne le nom de domaine d'origine, et non le nom de domaine de la distribution.

CloudFront Si l'`Host`en-tête contient le nom de domaine de la distribution, le point de terminaison renvoie une erreur HTTP 404 (introuvable). Si vous utilisez une politique de demande d'origine gérée, utilisez`AllViewerExceptHostHeader`, not`AllViewer`. Pour plus d'informations, consultez AllViewerExceptHostHeader.

> **Note**
>
> Les déclencheurs de demande d'origine et de réponse d'origine Lambda @Edge ne sont pas pris en charge dans les comportements de cache qui utilisent une origine de fonction Web Lambda avec OAC. Cela s'applique aux points de terminaison régionaux et mondiaux, ainsi qu'aux origines accessibles directement ou via un groupe d'origine. CloudFront rejette une configuration de distribution qui contient les deux.

Accorder CloudFront l'autorisation d'accéder à la fonction Web Lambda

Attachez une politique basée sur les ressources à la fonction Web Lambda qui permet au principal du CloudFront service (`cloudfront.amazonaws.com`) d'appeler le point de terminaison. L'action IAM pour appeler un point de terminaison est. `lambda:InvokeWebFunctionEndpoint` La politique est attachée à la fonction Web Lambda, mais chaque instruction peut l'étendre `Resource` à un ARN de point de terminaison spécifique. Utilisez un `Condition` élément pour autoriser l'accès CloudFront au point de terminaison uniquement lorsque la demande provient de la CloudFront distribution qui contient l'origine.

Example Resource-based politique de l' CloudFront OAC

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontOACAccess",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "lambda:InvokeWebFunctionEndpoint",
            "Resource": "arn:aws:lambda:us-east-1:111122223333:web-function/my-
function/endpoint/prod",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/EDFDVBD6EXAMPLE"
                }
            }
        }
    ]
}
```

Pour associer la politique basée sur les ressources, utilisez la put-resource-policy commande avec la fonction ARN (et non un ARN de point de terminaison) :

```
aws lambda-web put-resource-policy \
  --resource-arn "arn:aws:lambda:us-east-1:111122223333:web-function/my-function" \
  --policy file://policy.json \
  --region us-east-1
```

Vous pouvez revoir ou supprimer la politique à l'aide des delete-resource-policy commandes get-resource-policy et.

> **Note**
>
> Pour les points de terminaison qui s'étendent sur plusieurs régions, Lambda réplique les modifications de politique dans toutes les régions qui desservent le point de terminaison. Une politique nouvelle ou mise à jour peut prendre peu de temps pour entrer en vigueur dans chaque région. Pour plus d'informations, consultez la section Réplication et cohérence éventuelle dans le Guide du AWS Lambda développeur.

Création du contrôle d’accès d’origine

Pour créer un contrôle d'accès à l'origine (OAC), vous pouvez utiliser le Console de gestion AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un contrôle d’accès à l’origine

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.

2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur l'écran Créer un paramètre de contrôle, procédez comme suit :

    a. Dans le volet Détails, entrez un Nom et (éventuellement) une Description pour le contrôle d'accès à l'origine.

    b. Choisissez Lambda dans le menu déroulant Type d'origine. Ce type d'origine est utilisé à la fois pour les URL des fonctions Lambda et pour les fonctions Web Lambda.

    c. Si votre origine est un point de terminaison global (le nom d'hôte se termine par `.lambda-web.global.on.aws`), sélectionnez l'option Utiliser le protocole de signature SIGv4a. Pour un point de terminaison régional (le nom d'hôte se termine par `.lambda-web.`*`AWS-Region`*`.on.aws`), laissez cette option désactivée.

    d. Pour Comportement de signature, choisissez Toujours signer, préserver l'autorisation du spectateur. Cette option apparaît sous Signer les demandes (recommandé), qui est sélectionnée par défaut. Les origines des fonctions Web Lambda ne prennent en charge que ce comportement de signature. Pour plus d'informations, consultez Comportement de signature.

5. Cliquez sur Créer.

Pour ajouter un contrôle d'accès à l'origine à une origine de fonction Web Lambda dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution avec une origine de fonction Web Lambda à laquelle vous souhaitez ajouter l'OAC, puis cliquez sur l'onglet Origins.
3. Sélectionnez l'origine de la fonction Web Lambda à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Pour Accès d'origine, sélectionnez Paramètres de contrôle d'accès d'origine (recommandé).
5. Dans le menu déroulant Origin access control (Contrôle d'accès d'origine), choisissez l'OAC que vous souhaitez utiliser.
6. Cliquez sur Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine de la fonction Web Lambda.

CLI

Utilisez la commande create-origin-access-control. Pour un point de terminaison régional (le nom d'hôte se termine par `.lambda-web.`*`AWS-Region`*`.on.aws`), utilisez le protocole de `sigv4` signature :

```
aws cloudfront create-origin-access-control \
    --origin-access-control-config '{
        "Name": "my-lambda-web-oac",
        "Description": "OAC for Lambda Web Function origin",
        "SigningProtocol": "sigv4",
        "SigningBehavior": "always-amz-auth",
        "OriginAccessControlOriginType": "lambda"
    }'
```

Pour un point de terminaison global (le nom d'hôte se termine par `.lambda-web.global.on.aws`), utilisez le protocole de `sigv4a` signature :

```
aws cloudfront create-origin-access-control \
    --origin-access-control-config '{
        "Name": "my-lambda-web-global-oac",
        "Description": "OAC for global Lambda Web Function origin",
        "SigningProtocol": "sigv4a",
        "SigningBehavior": "always-amz-auth",
        "OriginAccessControlOriginType": "lambda"
    }'
```

CloudFormation

Spécifiez les valeurs suivantes dans `OriginAccessControlConfig` :

- `SigningProtocol`: `sigv4` (paramètre régional) ou `sigv4a` (paramètre global)
- `SigningBehavior`: `always-amz-auth`
- `OriginAccessControlOriginType`: `lambda`

Example CloudFormation modèle

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
    Description: An optional description for the origin access control
    Name: my-lambda-web-oac
    OriginAccessControlOriginType: lambda
    SigningBehavior: always-amz-auth
    SigningProtocol: sigv4a
```

Pour plus d'informations, voir AWS::CloudFront: : OriginAccessControl dans le guide de AWS CloudFormation l'utilisateur.

L'OAC ne prend effet pour chaque demande qu'une fois le déploiement de la distribution terminé. Pour un point de terminaison qui couvre plusieurs régions, la politique basée sur les ressources que vous avez attachée précédemment doit également terminer sa réplication dans chaque région qui dessert le point de terminaison. Tant que les deux ne sont pas terminées, certaines demandes peuvent recevoir une réponse HTTP 403 transitoire de la part de l'origine. Ces erreurs sont résolues automatiquement une fois le déploiement de la distribution terminé et la réplication de la politique terminée.

Comportement de signature

Les origines des fonctions Web Lambda ne prennent en charge que le comportement de `always-amz-auth` signature (toujours signer, préserver l'autorisation du lecteur dans la console). CloudFront signe toujours toutes les demandes qu'il envoie à la fonction Web Lambda, mais il ne remplace pas l'`Authorization`en-tête de la demande du visualiseur. Il CloudFront ajoute plutôt sa signature dans un CloudFront en-tête dédié et transmet l'`Authorization`en-tête du spectateur à l'origine sans modification. Avec ce comportement, votre fonction Web Lambda peut recevoir l'`Authorization`en-tête original du lecteur (par exemple, pour effectuer sa propre authentification ou autorisation). CloudFront signe toujours chaque demande qu'il envoie à l'origine. Pour transférer l'`Authorization`en-tête du visualiseur, vous devez l'ajouter à une politique de cache pour chaque comportement de cache utilisant l'origine.

Les autres comportements de signature (`always`ne`never`, et`no-override`) ne sont pas pris en charge pour les origines des fonctions Web Lambda. Le comportement de `always-amz-auth` signature n'est pris en charge pour aucun autre type d'origine, y compris les origines d'URL de la fonction Lambda.

For PUTPOST, et PATCH requests, CloudFront signe la demande d'origine avec une charge utile non signée ()UNSIGNED-PAYLOAD. Le corps de la demande n'est pas couvert par la CloudFront signature. La signature couvre toujours la méthode de demande, le chemin, la chaîne de requête et les en-têtes qui identifient votre distribution. Le point de terminaison peut donc vérifier que chaque demande provient CloudFront de votre distribution avant d'appeler votre fonction Web Lambda. Le corps de la demande est protégé en transit par la connexion HTTPS entre CloudFront et le point de terminaison. Il n'est pas nécessaire d'inclure un x-amz-content-sha256 en-tête dans les demandes adressées à CloudFront. Si un utilisateur en envoie une, il CloudFront ne l'utilise pas lors de la signature de la demande d'origine.

Restriction de l’accès à une origine Amazon S3

CloudFront propose deux méthodes pour envoyer des demandes authentifiées à une origine Amazon S3 : le contrôle d'accès à l'origine (OAC) et l'identité d'accès à l'origine (OAI). L’OAC vous permet de sécuriser vos origines, telles qu’Amazon S3.

Nous vous recommandons d’utiliser l’OAC à la place, car il prend en charge les fonctionnalités suivantes :

- Tous les compartiments Amazon S3 en tout Régions AWS, y compris les régions optionnelles lancées après décembre 2022
- Chiffrement côté serveur Amazon S3 avec AWS KMS () SSE-KMS
- Demandes dynamiques (PUT et DELETE) vers Amazon S3

L’OAI ne prend pas en charge ces fonctionnalités ou nécessite des solutions de contournement supplémentaires dans ces scénarios. Si vous utilisez déjà OAI et que vous souhaitez effectuer une migration, consultez the section called “Migration de l'identité d'accès à l'origine (OAI) vers le contrôle d'accès à l'origine (OAC)”.

Remarques

- Lorsque vous utilisez l' CloudFront OAC avec les origines des compartiments Amazon S3, vous devez définir Amazon S3 Object Ownership pour que le propriétaire du compartiment soit appliqué, ce qui est le cas par défaut pour les nouveaux compartiments Amazon S3. Si vous avez besoin d'ACL, utilisez le paramètre préféré du propriétaire du compartiment pour garder le contrôle sur les objets chargés à l'aide CloudFront de.

- Si votre origine est un compartiment Amazon S3 configuré comme point de terminaison de site Web, vous devez le configurer en CloudFront tant qu'origine personnalisée. Cela signifie que vous ne pouvez pas utiliser OAC (ou OAI). L'OAC ne prend pas en charge la redirection d'origine à l'aide de Lambda@Edge.
- Si vous utilisez un point d' Multi-Region accès Amazon S3 comme point CloudFront d'origine, consultezthe section called "Restreindre l'accès à l'origine d'un point Multi-Region d'accès Amazon S3". Les points Multi-Region d'accès S3 nécessitent une configuration OAC différente.

Les rubriques suivantes décrivent comment utiliser l'origine Amazon S3.

Rubriques

- the section called "Création d'un nouveau contrôle d'accès d'origine"
- the section called "Suppression d'une distribution avec un OAC associé à un compartiment S3"
- the section called "Migration de l'identité d'accès à l'origine (OAI) vers le contrôle d'accès à l'origine (OAC)"
- the section called "Paramètres avancés pour le contrôle d'accès à l'origine"

Création d'un nouveau contrôle d'accès d'origine

Suivez les étapes décrites dans les rubriques suivantes pour configurer un nouveau contrôle d'accès à l'origine dans CloudFront.

Rubriques

- Conditions préalables
- Accorder l' CloudFront autorisation d'accéder au compartiment S3
- Création du contrôle d'accès d'origine

Conditions préalables

Avant de créer et de configurer le contrôle d'accès à l'origine (OAC), vous devez disposer d'une CloudFront distribution avec une origine de compartiment Amazon S3. Cette origine doit être un compartiment S3 normal, et non un compartiment configuré en tant que point de terminaison.

Pour plus d'informations sur la configuration d'une CloudFront distribution avec une origine de compartiment S3, consultezthe section called “Mise en route avec une distribution standard”.

> **Important**
>
> Lorsque vous utilisez OAC pour sécuriser votre origine Amazon S3, la communication entre Amazon S3 CloudFront et Amazon S3 se fait toujours via HTTPS, mais uniquement lorsque vous choisissez de toujours signer les demandes. Vous devez choisir Signer les demandes (recommandé) dans la console ou les spécifier `always` dans l' CloudFront API AWS CLI, ou CloudFormation.
> Si vous choisissez plutôt l'option Ne pas signer les demandes ou Ne pas remplacer l'en-tête d'autorisation, utilisez le CloudFront protocole de connexion que vous avez spécifié dans les politiques suivantes :
>
> - Politique du protocole Viewer
> - Stratégie de protocole de l’origine (origines personnalisées uniquement)
>
> Par exemple, si vous choisissez Ne pas remplacer l'en-tête d'autorisation et que vous souhaitez utiliser le protocole HTTPS entre CloudFront et votre origine Amazon S3, utilisez Redirect HTTP vers HTTPS ou HTTPS uniquement pour la politique de protocole de visualisation.

Accorder l' CloudFront autorisation d'accéder au compartiment S3

Avant de créer un contrôle d'accès à l'origine (OAC) ou de le configurer dans une CloudFront distribution, assurez-vous que celui-ci CloudFront est autorisé à accéder à l'origine du compartiment S3. Procédez ainsi après avoir créé une CloudFront distribution, mais avant d'ajouter l'OAC à l'origine S3 dans la configuration de distribution.

Utilisez une politique de compartiment S3 pour autoriser le principal de CloudFront service (`cloudfront.amazonaws.com`) à accéder au compartiment. Utilisez un `Condition` élément de la politique CloudFront pour autoriser l'accès au compartiment uniquement lorsque la demande provient de la CloudFront distribution contenant l'origine S3. Il s’agit de la distribution contenant l’origine S3 à laquelle vous souhaitez ajouter l’OAC.

Pour plus d'informations sur l'ajout ou la modification d'une stratégie de compartiment, consultez Ajout d'une stratégie de compartiment à l'aide de la console Amazon S3 dans le Guide de l'utilisateur Amazon S3.

Voici des exemples de politiques de compartiment S3 qui autorisent une CloudFront distribution avec OAC à accéder à une origine S3.

Example Politique de compartiment S3 qui autorise l'accès en lecture seule pour une CloudFront distribution avec OAC activé

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipalReadOnly",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
        }
      }
    }
  ]
}
```

Example Politique de compartiment S3 qui autorise l'accès en lecture et en écriture pour une CloudFront distribution avec OAC activé

JSON

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipalReadWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID>"
        }
      }
    }
  ]
}
```

SSE-KMS

Si les objets de l'origine du compartiment S3 sont chiffrés à l'aide du chiffrement côté serveur avec AWS Key Management Service (SSE-KMS), vous devez vous assurer que la CloudFront distribution est autorisée à utiliser la AWS KMS clé. Pour autoriser la CloudFront distribution à utiliser la clé KMS, ajoutez une déclaration à la politique de clé KMS. Pour plus d'informations sur la modification d'une stratégie de clé, consultez Modification d'une stratégie de clé dans le Guide du développeur AWS Key Management Service .

Example Déclaration de stratégie de clé KMS

L'exemple suivant montre une déclaration AWS KMS de politique qui permet à la CloudFront distribution avec OAC d'accéder à une clé KMS pour SSE-KMS.

```
{
    "Sid": "AllowCloudFrontServicePrincipalSSE-KMS",
    "Effect": "Allow",
    "Principal": {
        "Service": [
```

```
            "cloudfront.amazonaws.com"
        ]
     },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
            "StringEquals": {
                "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
            }
        }
}
```

Création du contrôle d’accès d’origine

Pour créer un contrôle d'accès à l'origine (OAC), vous pouvez utiliser le Console de gestion AWS CloudFormation, AWS CLI, ou l' CloudFront API.

Console

Pour créer un contrôle d’accès à l’origine

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur l'écran Créer un paramètre de contrôle, procédez comme suit :
    a. Dans le volet Détails, entrez un Nom et (éventuellement) une Description pour le contrôle d'accès à l'origine.
    b. Dans le volet Paramètres, nous vous recommandons de conserver le paramètre par défaut (Signer les demandes (recommandé)). Pour plus d’informations, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.
5. Choisissez S3 dans la liste déroulante Origin type (Type de l'origine).
6. Cliquez sur Créer.

Après avoir créé l'OAC, prenez note de Nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un contrôle d'accès à une origine S3 dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution avec une origine S3 à laquelle vous souhaitez ajouter l'OAC, puis choisissez l'onglet Origines.
3. Sélectionnez l'origine S3 que vous souhaitez ajouter à l'origine, puis choisissez Modifier.
4. Pour Accès d'origine, sélectionnez Paramètres de contrôle d'accès d'origine (recommandé).
5. Dans le menu déroulant Origin access control (Contrôle d'accès d'origine), choisissez l'OAC que vous souhaitez utiliser.
6. Cliquez sur Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine du compartiment S3.

CloudFormation

Pour créer un contrôle d'accès à l'origine (OAC) avec CloudFormation, utilisez le type de `AWS::CloudFront::OriginAccessControl` ressource. L'exemple suivant montre la syntaxe du CloudFormation modèle, au format YAML, pour créer un contrôle d'accès à l'origine.

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
      Description: An optional description for the origin access control
      Name: ExampleOAC
      OriginAccessControlOriginType: s3
      SigningBehavior: always
      SigningProtocol: sigv4
```

Pour plus d'informations, voir AWS::CloudFront: : OriginAccessControl dans le guide de AWS CloudFormation l'utilisateur.

CLI

Pour créer un contrôle d'accès à l'origine avec le AWS Command Line Interface (AWS CLI), utilisez la aws cloudfront create-origin-access-control commande. Vous pouvez utiliser un fichier d'entrée pour fournir les paramètres d'entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer un contrôle d'accès à l'origine (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `origin-access-control.yaml`. Ce fichier contient tous les paramètres d'entrée de la commande create-origin-access-control.

```
aws cloudfront create-origin-access-control --generate-cli-skeleton yaml-input >
 origin-access-control.yaml
```

2. Ouvrez le fichier `origin-access-control.yaml` que vous venez de créer. Modifiez le fichier pour ajouter un nom à l'OAC, une description (facultative) et remplacez `SigningBehavior` par `always`. Ensuite, enregistrez le fichier.

   Pour plus d'informations sur paramètres OAC, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.

3. Utilisez la commande suivante pour créer le contrôle d'accès à l'origine à l'aide des paramètres d'entrée du fichier `origin-access-control.yaml`.

```
aws cloudfront create-origin-access-control --cli-input-yaml file://origin-
access-control.yaml
```

   Notez la valeur de `Id` dans la sortie de la commande. Vous en avez besoin pour ajouter l'OAC à l'origine d'un compartiment S3 dans une CloudFront distribution.

Pour attacher un OAC à l'origine d'un compartiment S3 dans une distribution existante (CLI avec un fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution à laquelle vous souhaitez ajouter l'OAC. La distribution doit avoir une origine de compartiment S3.

```
aws cloudfront get-distribution-config --id <CloudFront distribution ID> --
output yaml > dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes :

   - Dans l'objet `Origins`, ajoutez l'ID de l'OAC au champ nommé `OriginAccessControlId`.
   - Supprimez la valeur du champ nommé `OriginAccessIdentity`, le cas échéant.
   - Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser le contrôle d'accès à l'origine.

```
aws cloudfront update-distribution --id <CloudFront distribution ID> --cli-
input-yaml file://dist-config.yaml
```

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine du compartiment S3.

API

Pour créer un contrôle d'accès à l'origine avec l' CloudFront API, utilisez CreateOriginAccessControl. Pour plus d'informations sur les champs que vous spécifiez dans cet appel d'API, consultez la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé un contrôle d'accès à l'origine, vous pouvez l'attacher à l'origine d'un compartiment S3 dans une distribution, à l'aide de l'un des appels d'API suivants :

- Pour l'associer à une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux appels d'API, indiquez l'ID de contrôle d'accès à l'origine dans le champ `OriginAccessControlId`, à l'intérieur d'une origine. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence de tous les paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Suppression d’une distribution avec un OAC associé à un compartiment S3

Si vous devez supprimer une distribution avec un OAC associé à un compartiment S3, vous devez supprimer la distribution avant de supprimer l’origine du compartiment S3. Vous pouvez également inclure la région dans le nom de domaine d’origine. Si cela n’est pas possible, vous pouvez supprimer l’OAC de la distribution en passant au mode public avant de le supprimer. Pour plus d’informations, consultez Supprimer une distribution.

Migration de l'identité d'accès à l'origine (OAI) vers le contrôle d'accès à l'origine (OAC)

Pour migrer d’une ancienne identité d’accès d’origine (OAI) vers un contrôle d’accès d’origine (OAC), commencez par mettre à jour l’origine du compartiment S3 afin de permettre à l’OAI et à la distribution avec OAC d’accéder au contenu du compartiment. Cela permet de ne CloudFront jamais perdre l'accès au bucket pendant la transition. Pour permettre à l’OAI et à la distribution avec OAC d’accéder à un compartiment S3, mettez à jour la Stratégie de compartiment de façon à inclure deux déclarations, une pour chaque type de principal.

L’exemple de stratégie de compartiment S3 suivant permet à la fois à une OAI et à une distribution avec OAC d’accéder à une origine S3.

Example Politique de compartiment S3 qui autorise l'accès en lecture seule à un OAI et à une CloudFront distribution avec OAC activé

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipalReadOnly",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
```

```
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/<CloudFront distribution ID>"
                }
            }
        },
        {
            "Sid": "AllowLegacyOAIReadOnly",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Après avoir mis à jour la stratégie de compartiment de l'origine S3 pour autoriser l'accès à la fois à l'OAI et à l'OAC, vous pouvez mettre à jour la configuration de distribution pour utiliser l'OAC au lieu de l'OAI. Pour plus d'informations, consultez the section called “Création d'un nouveau contrôle d'accès d'origine”.

Une fois la distribution entièrement déployée, vous pouvez supprimer l'instruction de la politique de compartiment qui autorise l'accès à l'OAI. Pour plus d'informations, consultez the section called “Accorder l' CloudFront autorisation d'accéder au compartiment S3”.

Paramètres avancés pour le contrôle d'accès à l'origine

La fonctionnalité de contrôle CloudFront d'accès à l'origine inclut des paramètres avancés destinés uniquement à des cas d'utilisation spécifiques. Utilisez les paramètres recommandés, sauf si vous avez des besoins spécifiques en matière de paramètres avancés.

Le contrôle d'accès à Origin contient un paramètre nommé Comportement de signature (dans la console) ou `SigningBehavior` (dans l'API, la CLI et CloudFormation). Ce paramètre fournit les options suivantes :

Toujours signer les demandes d'origine (paramètre recommandé)

Nous vous recommandons d’utiliser ce paramètre, nommé Signer les demandes (recommandé) dans la console ou `always` dans l’API, la CLI et CloudFormation. Avec ce paramètre, il signe CloudFront toujours toutes les demandes qu'il envoie à l'origine du compartiment S3.

Ne jamais signer les demandes d’origine

Ce paramètre est nommé Ne pas signer les demandes dans la console ou `never` dans l'API, la CLI et CloudFormation. Utilisez ce paramètre pour désactiver le contrôle d'accès à l'origine pour toutes les origines dans toutes les distributions qui utilisent ce contrôle d'accès à l'origine. Cela permet d’économiser du temps et des efforts par rapport à la suppression d’un contrôle d’accès à l’origine de toutes les origines et distributions qui l’utilisent, une par une. Avec ce paramètre, il CloudFront ne signe aucune demande envoyée à l'origine du compartiment S3.

> **Warning**
>
> Pour utiliser ce paramètre, l'origine du compartiment S3 doit être accessible au public. Si vous utilisez ce paramètre avec une origine de compartiment S3 qui n'est pas accessible au public, vous CloudFront ne pouvez pas accéder à l'origine. L'origine du compartiment S3 renvoie les erreurs aux utilisateurs CloudFront et les CloudFront transmet aux utilisateurs.

Ne remplacez pas l’en-tête **`Authorization`** de l’utilisateur (client)

Ce paramètre est nommé Ne pas remplacer l'en-tête d'autorisation dans la console ou `no-override` dans l'API, la CLI et CloudFormation. Utilisez ce paramètre lorsque vous CloudFront souhaitez signer des demandes d'origine uniquement lorsque la demande d'affichage correspondante ne contient pas d'`Authorization`en-tête. Avec ce paramètre, CloudFront transmet l'`Authorization`en-tête de la demande du visualiseur lorsqu'il y en a un, mais signe la demande d'origine (en ajoutant son propre `Authorization` en-tête) lorsque la demande du visualiseur n'inclut pas d'`Authorization`en-tête.

> **Warning**
>
> Pour parcourir l'en-tête `Authorization` de la demande de l'utilisateur, vous devez ajouter l'en-tête `Authorization` à une stratégie de mise en cache pour tous les

comportements de cache qui utilisent les origines du compartiment S3 associées à ce contrôle d'accès à l'origine.

Utilisation d’une identité d’accès d’origine (héritée, non recommandée)

Présentation de l'identité d'accès à l'origine

CloudFront L'identité d'accès à l'origine (OAI) fournit des fonctionnalités similaires à celles du contrôle d'accès à l'origine (OAC), mais elle ne fonctionne pas dans tous les scénarios. Plus précisément, l'OAI ne prend pas en charge :

- Tous les compartiments Amazon S3 Régions AWS, y compris les régions optionnelles
- Chiffrement côté serveur Amazon S3 avec AWS KMS () SSE-KMS
- Demandes dynamiques (`PUT`, `POST` ou `DELETE`) vers Amazon S3
- Nouveau Régions AWS produit lancé après janvier 2023

> **Tip**
>
> Nous vous recommandons d’utiliser l’OAC à la place. Pour configurer l’OAC, consultez Création d’un nouveau contrôle d’accès d’origine. Pour plus d'informations sur la migration d'OAI vers OAC, consultez the section called “Migration de l'identité d'accès à l'origine (OAI) vers le contrôle d'accès à l'origine (OAC)”.

Attribution à l’identité d’accès d’origine de l’autorisation de lire les fichiers du compartiment Amazon S3

Lorsque vous créez un OAI ou que vous en ajoutez un à une distribution à l'aide de la CloudFront console, vous pouvez automatiquement mettre à jour la politique de compartiment Amazon S3 pour autoriser l'OAI à accéder à votre compartiment. Vous pouvez également choisir de créer ou de mettre à jour manuellement la politique de compartiment. Quelle que soit la méthode que vous utilisez, vous devez toujours vérifier les autorisations pour vous assurer que :

- Votre CloudFront OAI peut accéder aux fichiers du bucket pour le compte des utilisateurs qui les demandent. CloudFront

- Les utilisateurs ne peuvent pas utiliser les URL Amazon S3 pour accéder à vos fichiers en dehors de CloudFront.

> **Important**
>
> Si vous configurez CloudFront pour accepter et transférer toutes les méthodes HTTP compatibles, CloudFront assurez-vous d'accorder à votre CloudFront OAI les autorisations souhaitées. Par exemple, si vous configurez CloudFront pour accepter et transférer les demandes qui utilisent cette `DELETE` méthode, configurez votre politique de compartiment de manière à gérer les `DELETE` demandes de manière appropriée afin que les utilisateurs puissent supprimer uniquement les fichiers que vous souhaitez qu'ils souhaitent.

Utilisation des stratégies de compartiment Amazon S3

Vous pouvez accorder à un CloudFront OAI l'accès aux fichiers d'un compartiment Amazon S3 en créant ou en mettant à jour la politique de compartiment de la manière suivante :

- Utilisation de l'onglet Autorisations du compartiment Amazon S3 dans la console Amazon S3.
- Utilisation PutBucketPolicydans l'API Amazon S3.
- En utilisant la console CloudFront. Lorsque vous ajoutez un OAI à vos paramètres d'origine dans la CloudFront console, vous pouvez choisir Oui, mettre à jour la politique de compartiment pour indiquer de mettre CloudFront à jour la politique de compartiment en votre nom.

Si vous mettez à jour manuellement la politique de compartiment, assurez-vous que vous :

- Spécifiez l'identité d'accès à l'origine correcte comme `Principal` dans la politique.
- Accordez à l'identité d'accès à l'origine les autorisations dont elle a besoin pour accéder aux objets pour le compte des utilisateurs.

Pour plus d'informations, consultez les sections suivantes.

Spécifier un OAI comme **`principal`** dans une politique de bucket

Pour spécifier une OAI comme `Principal` dans une politique de compartiment Amazon S3, utilisez l'Amazon Resource Name (ARN) qui inclut son ID. Par exemple :

```
"Principal": {
    "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <origin
 access identity ID>"
}
```

Trouvez l'ID OAI dans la CloudFront console sous Security, Origin access, Identities (legacy). Vous pouvez également l'utiliser ListCloudFrontOriginAccessIdentitiesdans l' CloudFrontAPI.

Octroi d’autorisations à une OAI

Pour donner à l’identité d’accès à l’origine les autorisations pour accéder aux objets de votre compartiment Amazon S3, utilisez des actions dans la politique qui se rapportent à des opérations d’API Amazon S3 spécifiques. Par exemple, l'action `s3:GetObject` permet à l'identité d'accès à l'origine de lire des objets dans le compartiment. Pour plus d’informations, consultez les exemples de la section suivante ou la section Actions Amazon S3 du Guide de l’utilisateur Amazon Simple Storage Service.

Exemples de politique de compartiment Amazon S3

Les exemples suivants présentent les politiques de compartiment Amazon S3 qui permettent à CloudFront OAI d'accéder à un compartiment S3.

Trouvez l'ID OAI dans la CloudFront console sous Security, Origin access, Identities (legacy). Vous pouvez également l'utiliser ListCloudFrontOriginAccessIdentitiesdans l' CloudFrontAPI.

Example Politique de compartiment Amazon S3 qui donne à l’identité d’accès à l’origine un accès en lecture

L’exemple suivant permet à l’identité d’accès à l’origine de lire des objets dans le compartiment spécifié (`s3:GetObject`).

JSON

```
{
    "Version":"2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Example Politique de compartiment Amazon S3 qui donne à l'identité d'accès à l'origine un accès en lecture et en écriture

L'exemple suivant permet à l'identité d'accès à l'origine de lire et d'écrire des objets dans le compartiment spécifié (`s3:GetObject` et `s3:PutObject`). Cela permet aux utilisateurs de télécharger des fichiers dans votre compartiment Amazon S3 via CloudFront.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity <origin access identity ID>"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::<S3 bucket name>/*"
        }
    ]
}
```

Utilisation des listes ACL d'objet Amazon S3 (non recommandée)

> **Important**
>
> Il est recommandé d'utiliser les politiques du compartiment Amazon S3 pour attribuer à une OAI l'accès à un compartiment S3. Vous pouvez utiliser des listes de contrôle d'accès (ACL) comme décrit dans cette section, mais nous le déconseillons.
> Amazon S3 recommande de définir S3 Object Ownership (Propriété de l'objet S3) sur bucket owner enforced (appliqué par le propriétaire du compartiment), ce qui signifie que les listes ACL sont désactivées pour le compartiment et les objets à l'intérieur. Lorsque vous appliquez ce paramètre à Object Ownership (Propriété de l'objet), vous devez utiliser des politiques du compartiment pour donner l'accès à l'OAI (consultez la section précédente).
> La section suivante concerne uniquement les cas d'utilisation hérités nécessitant des listes ACL.

Vous pouvez accorder à un CloudFront OAI l'accès aux fichiers d'un compartiment Amazon S3 en créant ou en mettant à jour l'ACL du fichier de la manière suivante :

- Utilisation de l'onglet Autorisations de l'objet Amazon S3 dans la console Amazon S3.
- Utilisation PutObjectAcldans l'API Amazon S3.

Lorsque vous accordez l'accès à une identité d'accès à l'origine à l'aide d'une liste ACL, vous devez spécifier l'identité d'accès à l'origine à l'aide de son ID d'utilisateur canonique Amazon S3. Dans la CloudFront console, vous pouvez trouver cet identifiant sous Sécurité, Accès à l'origine, Identités (ancienne). Si vous utilisez l' CloudFront API, utilisez la valeur de l'`S3CanonicalUserId`élément renvoyé lorsque vous avez créé l'OAI, ou appelez ListCloudFrontOriginAccessIdentitiesl' CloudFrontAPI.

Utilisation d'une identité d'accès d'origine dans les régions Amazon S3 prenant uniquement en charge l'authentification Signature version 4

Les régions Amazon S3 plus récentes requièrent que vous utilisiez Signature version 4 pour les demandes authentifiées. (Pour connaître les versions de signatures prises en charge dans chaque région Amazon S3, consultez la section Points de terminaison et quotas Amazon Simple Storage Service de la Références générales AWS.) Si vous utilisez une identité d'accès à l'origine et que votre compartiment se trouve dans l'une des régions qui nécessitent Signature version 4, notez les points suivants :

- Les demandes `DELETE`, `GET`, `HEAD`, `OPTIONS` et`PATCH` sont prises en charge sans qualifications.
- Les demandes `POST` ne sont pas prises en charge.

Restriction de l’accès avec les origines de VPC

Vous pouvez l'utiliser CloudFront pour diffuser du contenu à partir d'applications hébergées dans les sous-réseaux privés de votre cloud privé virtuel (VPC). Vous pouvez utiliser des Application Load Balancers (ALB), des Network Load Balancers (NLB) et des instances EC2 dans des sous-réseaux privés en tant qu’origines VPC.

Voici certaines raisons pour lesquelles vous pourriez choisir d’utiliser des origines VPC :

- Sécurité : VPC Origins est conçu pour améliorer le niveau de sécurité de votre application en plaçant vos équilibreurs de charge et vos instances EC2 dans des sous-réseaux privés, constituant CloudFront ainsi un point d'entrée unique. Les demandes des utilisateurs sont CloudFront transmises aux origines du VPC via une connexion privée et sécurisée, ce qui renforce la sécurité de vos applications.
- Gestion — Les origines des VPC réduisent la charge opérationnelle requise pour sécuriser la connectivité entre les origines CloudFront et les origines. Vous pouvez déplacer vos origines vers des sous-réseaux privés sans accès public, sans avoir à implémenter de listes de contrôle d’accès (ACL) ou d’autres mécanismes pour restreindre l’accès à vos origines. Ainsi, vous n'avez pas à investir dans un travail de développement indifférencié pour sécuriser vos applications Web. CloudFront
- Évolutivité et performances : les origines du VPC vous aident à sécuriser vos applications Web, ce qui vous permet de vous concentrer sur le développement de vos applications professionnelles critiques tout en améliorant la sécurité et en maintenant des performances élevées et une évolutivité mondiale grâce à. CloudFront Les origines du VPC rationalisent la gestion de la sécurité et réduisent la complexité opérationnelle afin que vous puissiez l'utiliser CloudFront comme point d'entrée unique pour vos applications.

> **Tip**
>
> CloudFront prend en charge le partage des origines des VPC Comptes AWS, qu'ils appartiennent ou non à votre organisation. Vous pouvez partager les origines des VPC

depuis la CloudFront console ou utiliser AWS Resource Access Manager ()AWS RAM. Pour plus d'informations, consultez Travailler avec des ressources partagées dans CloudFront.

Conditions préalables

Avant de créer une origine VPC pour votre CloudFront distribution, vous devez effectuer les opérations suivantes :

VPC Configuration

Créez un cloud privé virtuel (VPC) sur Amazon VPC dans l'un des clouds pris en charge pour Régions AWS les origines de VPC. Pour en savoir plus sur la création d'un VPC, consultez Créer un VPC et d'autres ressources VPC dans le Guide de l'utilisateur Amazon VPC. Pour obtenir une liste des régions prises en charge, consultez Pris en charge Régions AWS pour les origines du VPC.

Votre VPC doit inclure les éléments suivants :

- Passerelle Internet : vous devez ajouter une passerelle Internet au VPC qui contient vos ressources d'origine VPC. La passerelle Internet est nécessaire pour indiquer que le VPC peut recevoir du trafic provenant d'Internet. La passerelle Internet n'est pas utilisée pour acheminer le trafic vers les origines du sous-réseau, et il n'est pas nécessaire de mettre à jour les politiques de routage.
- Sous-réseau privé avec au moins une adresse IPv4 disponible (et, pour la prise en charge de la double pile, au moins une adresse IPv6 disponible) : CloudFront route vers votre sous-réseau à l'aide d'une interface ELASTIC network (ENI CloudFront) gérée par des services qui est créée une fois que vous avez défini votre ressource d'origine VPC. Vous devez disposer d'au moins une adresse IPv4 disponible (et, pour la prise en charge de la double pile, d'au moins une adresse IPv6 disponible) dans votre sous-réseau privé afin que le processus de création de l'ENI puisse réussir. Ces adresses peuvent être privées, sans frais supplémentaires.

Ressources d'origine

Dans le sous-réseau privé, déployez un Application Load Balancer, un Network Load Balancer ou une instance EC2 qui servira d'origine. La ressource que vous lancez doit être entièrement déployée et présenter l'état Actif avant de pouvoir être utilisée comme origine VPC.

Restrictions d'origine :

- Les équilibreurs de charge Gateway ne peuvent pas être ajoutés en tant qu'origines
- Les équilibreurs de charge réseau dotés d'écouteurs TLS ne peuvent pas être ajoutés en tant qu'origines
- Pour être utilisé comme origine VPC, un Network Load Balancer doit être associé à un groupe de sécurité

Configuration du groupe de sécurité

Un groupe de sécurité doit être attaché à vos ressources d'origine VPC (Application Load Balancer, Network Load Balancer ou instance EC2). Lorsque vous créez une origine VPC, un groupe de sécurité géré par des services est CloudFront automatiquement créé avec le modèle de dénomination. `CloudFront-VPCOrigins-Service-SG` Ce groupe de sécurité est entièrement géré par AWS et ne doit pas être modifié.

Pour autoriser le trafic en provenance de votre VPC CloudFront à atteindre l'origine, mettez à jour le groupe de sécurité attaché à votre ressource d'origine (instance ALB, NLB ou EC2) afin d'autoriser le trafic entrant en utilisant l'une des méthodes suivantes :

- Option 1 : Autoriser le trafic depuis la liste des préfixes CloudFront gérés. Pour plus d'informations, consultez Utiliser la liste de préfixes CloudFront gérée. Cela peut également être fait avant la création de l'origine du VPC. Pour une origine VPC IPv4, utilisez uniquement. `com.amazonaws.global.cloudfront.origin-facing` Pour une origine VPC à double pile, utilisez `com.amazonaws.global.cloudfront.origin-facing` à la fois et. `com.amazonaws.global.ipv6.cloudfront.origin-facing`
- Option 2 : autoriser le trafic provenant du groupe de sécurité CloudFront géré par le service ()`CloudFront-VPCOrigins-Service-SG`. Cela ne peut être fait qu'une fois l'origine du VPC créée et le groupe de sécurité géré par le service créé. Cette configuration est encore plus restrictive car elle restreint le trafic uniquement à vos CloudFront distributions.

> **Important**
>
> Ne créez pas votre propre groupe de sécurité dont le nom commence par`CloudFront-VPCOrigins-Service-SG`. Il s'agit d'un modèle de dénomination AWS réservé aux groupes de sécurité gérés par des services. Pour plus d'informations, consultez Création d'un groupe de sécurité.

Restrictions relatives au protocole et aux fonctionnalités

Les origines VPC ne prennent pas en charge les éléments suivants :

- Trafic gRPC
- Déclencheurs de demande d'origine et de réponse d'origine avec Lambda @Edge
- Listes de contrôle d'accès réseau (NACL) : les règles NACL entrantes ne sont pas évaluées pour le trafic en provenance de CloudFront votre VPC d'origine. Cependant, les règles NACL sortantes sont évaluées sur le chemin de retour et doivent autoriser le trafic sur les ports TCP éphémères (1024 à 65535) vers ou vers les plages d'adresses IP orientées vers l'origine. `0.0.0.0/0` CloudFront

Création d’une origine VPC (nouvelle distribution)

La procédure suivante explique comment créer une origine VPC pour votre nouvelle CloudFront distribution dans la CloudFront console. Vous pouvez également utiliser les opérations d'CreateDistributionAPI CreateVpcOrigineet avec le AWS CLI ou un AWS SDK.

Pour créer une origine VPC pour une nouvelle distribution CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez les Origines du VPC, puis Créer une origine du VPC.
3. Renseignez les champs obligatoires. Pour ARN d’origine, sélectionnez l’ARN de votre Application Load Balancer, un Network Load Balancer ou une instance EC2. Si l’ARN n’apparaît pas, copiez l’ARN de votre ressource et collez-le ici.
4. Sélectionnez le type d'origine. La valeur par défaut est IPv4.
5. Choisissez Créer une origine du VPC.
6. Attendez que l’état de l’origine VPC passe à Déployé. Ce processus peut prendre jusqu’à 15 minutes.
7. Choisissez Distributions, puis Créer une distribution.
8. Pour Domaine de l’origine, sélectionnez la ressource de l’origine VPC dans la liste déroulante.

   Si votre origine VPC est une instance EC2, copiez et collez le Nom DNS IP privé de l’instance dans le champ Domaine de l’origine.
9. Terminez la création de votre distribution. Pour plus d’informations, consultez Création d'une CloudFront distribution dans la console.

Création d'une origine VPC (distribution existante)

La procédure suivante explique comment créer une origine VPC pour votre CloudFront distribution existante dans la CloudFront console, afin de garantir la disponibilité continue de vos applications. Vous pouvez également utiliser les opérations d'UpdateDistributionWithStagingConfigAPI CreateVpcOriginet avec le AWS CLI ou un AWS SDK.

Vous pouvez éventuellement choisir d'ajouter l'origine VPC à votre distribution existante sans créer de distribution intermédiaire.

Pour créer une origine VPC pour votre distribution existante CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez les Origines du VPC, puis Créer une origine du VPC.
3. Renseignez les champs obligatoires. Pour ARN d'origine, sélectionnez l'ARN de votre Application Load Balancer, un Network Load Balancer ou une instance EC2. Si l'ARN n'apparaît pas, copiez l'ARN de votre ressource et collez-le ici.
4. Sélectionnez le type d'origine. La valeur par défaut est IPv4.
5. Choisissez Créer une origine du VPC.
6. Attendez que l'état de l'origine VPC passe à Déployé. Ce processus peut prendre jusqu'à 15 minutes.
7. Dans le volet de navigation, sélectionnez Distributions.
8. Choisissez l'ID de votre distribution.
9. Dans l'onglet Questions d'ordre général, sous Déploiement continu, choisissez Créer une distribution intermédiaire. Pour plus d'informations, consultez Utilisez le déploiement CloudFront continu pour tester en toute sécurité les modifications de configuration du CDN.
10. Suivez les étapes de l'assistant indiquées dans Créer une distribution intermédiaire pour créer une distribution intermédiaire. Effectuez les étapes suivantes :

    - Pour Origines, choisissez Créer une origine.
    - Pour Domaine de l'origine, sélectionnez la ressource de votre origine VPC dans le menu déroulant.

      Si votre origine VPC est une instance EC2, copiez et collez le Nom DNS IP privé de l'instance dans le champ Domaine de l'origine.
    - Choisissez Create origin (Créer une origine).

11. Dans votre distribution intermédiaire, testez l'origine VPC.
12. Faites passer la configuration de distribution intermédiaire à votre distribution principale. Pour plus d'informations, consultez Promouvoir la configuration d'une distribution intermédiaire.
13. Supprimez l'accès public à votre origine VPC en rendant le sous-réseau privé. Une fois cela fait, l'origine du VPC ne sera plus détectable sur Internet, mais CloudFront vous aurez toujours un accès privé à celui-ci. Pour plus d'informations, consultez Associer ou dissocier un sous-réseau à une table de routage dans le Guide de l'utilisateur Amazon VPC.

Mise à jour d'une origine VPC

La procédure suivante explique comment mettre à jour une origine VPC pour votre CloudFront distribution dans la CloudFront console. Vous pouvez également utiliser les opérations d'UpdateVpcOriginAPI UpdateDistributionet avec le AWS CLI ou un AWS SDK.

Pour mettre à jour une origine VPC existante pour votre distribution CloudFront

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Distributions.
3. Choisissez l'ID de votre distribution.
4. Choisissez l'onglet Comportements.
5. Assurez-vous que l'origine VPC n'est pas l'origine par défaut de votre comportement de cache.
6. Choisissez l'onglet Origines.
7. Sélectionnez l'origine VPC que vous souhaitez mettre à jour et choisissez Supprimer. Cette opération dissocie l'origine VPC de votre distribution. Répétez les étapes 2 à 7 pour dissocier l'origine VPC de toute autre distribution.
8. Choisissez Origines du VPC.
9. Sélectionnez l'origine VPC et choisissez Modifier.
10. Effectuez vos mises à jour et choisissez Mettre à jour l'origine du VPC.
11. Attendez que l'état de l'origine VPC passe à Déployé. Ce processus peut prendre jusqu'à 15 minutes.
12. Dans le volet de navigation, sélectionnez Distributions.
13. Choisissez l'ID de votre distribution.
14. Choisissez l'onglet Origines.
15. Choisissez Create origin (Créer une origine).

16. Pour Domaine de l’origine, sélectionnez la ressource de votre origine VPC dans le menu déroulant.

    Si votre origine VPC est une instance EC2, copiez et collez le Nom DNS IP privé de l’instance dans le champ Domaine de l’origine.

17. Choisissez Create origin (Créer une origine). Cette opération associe à nouveau l’origine VPC à votre distribution. Répétez les étapes 12 à 17 pour associer l’origine VPC mise à jour à toute autre distribution.

Pris en charge Régions AWS pour les origines du VPC

Les origines VPC sont actuellement prises en charge dans la publicité suivante. Régions AWS Les exceptions de zone de disponibilité (AZ) sont notées.

Nom de la région	Région
US East (Ohio)	`us-east-2`
USA Est (Virginie du Nord)	`us-east-1 (except AZ use1-az3)`
USA Ouest (Californie du Nord)	`us-west-1 (except AZ usw1-az2)`
USA Ouest (Oregon)	`us-west-2`
Afrique (Le Cap)	`af-south-1`
Asie-Pacifique (Hong Kong)	`ap-east-1`
Asie-Pacifique (Mumbai)	`ap-south-1`
Asie-Pacifique (Hyderabad)	`ap-south-2`
Asie-Pacifique (Jakarta)	`ap-southeast-3`
Asie-Pacifique (Melbourne)	`ap-southeast-4`
Asie-Pacifique (Osaka)	`ap-northeast-3`
Asie-Pacifique (Singapour)	`ap-southeast-1`

Nom de la région	Région
Asie-Pacifique (Sydney)	`ap-southeast-2`
Asia Pacific (Tokyo)	`ap-northeast-1 (except AZ apne1-az3)`
Asie-Pacifique (Séoul)	`ap-northeast-2`
Asie-Pacifique (Thaïlande)	`ap-southeast-7`
Asie-Pacifique (Malaisie)	`ap-southeast-5`
Asie-Pacifique (Nouvelle Zélande)	`ap-southeast-6`
Asie-Pacifique (Taipei)	`ap-east-2`
Canada (Centre)	`ca-central-1 (except AZ cac1-az3)`
Canada-Ouest (Calgary)	`ca-west-1`
Europe (Francfort)	`eu-central-1`
Europe (Irlande)	`eu-west-1`
Europe (Londres)	`eu-west-2`
Europe (Milan)	`eu-south-1`
Europe (Paris)	`eu-west-3`
Europe (Espagne)	`eu-south-2`
Europe (Stockholm)	`eu-north-1`
Europe (Zurich)	`eu-central-2`
Israël (Tel Aviv)	`il-central-1`
Middle East (Bahrain)	`me-south-1`
Moyen-Orient (EAU)	`me-central-1`

Nom de la région	Région
Amérique du Sud (São Paulo)	`sa-east-1`
Mexique (Centre)	`mx-central-1`

Restreindre l'accès à l'origine d'un point Multi-Region d'accès Amazon S3

Vous pouvez utiliser le contrôle d'accès à l'origine (OAC) pour restreindre l'accès à une origine Amazon S3 Multi-Region Access Point. Les points Multi-Region d'accès S3 fournissent un point de terminaison global qui achemine les demandes vers le compartiment S3 le plus proche en fonction de la latence du réseau.

> **Note**
>
> L'OAC avec points Multi-Region d'accès S3 n'est pas pris en charge pour les points de terminaison MRAP soutenus par des compartiments dans les régions optionnelles. Les demandes acheminées vers un bucket situé dans une région optionnelle échoueront. Tous les compartiments associés au point Multi-Region d'accès doivent se trouver dans des régions activées par défaut.

Pour plus d'informations sur l'utilisation de l'OAC avec l'origine d'un compartiment Amazon S3 standard, consultezthe section called “Restriction de l’accès à une origine Amazon S3”.

Conditions préalables

Avant de créer et de configurer l'OAC, vous devez disposer d'une CloudFront distribution ayant pour origine un point d' Multi-Region accès Amazon S3. Le nom de domaine d'origine doit utiliser le format de nom d'hôte S3 Multi-Region Access Point :

```
multi-region-access-point-alias.accesspoint.s3-global.amazonaws.com
```

Pour plus d'informations sur la création d'un point d' Multi-Region accès S3, consultez la section Création de points Multi-Region d'accès dans le guide de l'utilisateur d'Amazon Simple Storage Service.

CloudFront Autoriser l'accès au point Multi-Region d'accès S3

Mettez à jour la politique du point d' Multi-Region accès pour permettre au principal du CloudFront service (`cloudfront.amazonaws.com`) d'accéder au point Multi-Region d'accès. Utilisez un `Condition` élément de la politique CloudFront pour autoriser l' Multi-Region accès au point d'accès uniquement lorsque la demande provient de la CloudFront distribution qui contient l'origine.

Pour plus d'informations sur l'ajout ou la modification d'une Multi-Region politique de point d'Multi-Regionaccès, consultez des exemples de politiques de point d'accès dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Example Multi-Region Politique relative aux points d'accès pour l' CloudFront OAC

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontOACAccess",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3::111122223333:accesspoint/Multi-Region-Access-
Point-Alias.mrap/object/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront distribution ID"
                }
            }
        }
    ]
}
```

Accorder CloudFront l'autorisation d'accéder aux compartiments S3 sous-jacents

Outre la politique de point Multi-Region d'accès, vous devez également CloudFront autoriser l'accès à chacun des compartiments S3 sous-jacents associés au point Multi-Region d'accès. Vous pouvez effectuer cette opération de deux manières :

> **Important**
>
> Vous devez ajouter cette politique de compartiment à chaque compartiment S3 associé au point Multi-Region d'accès. Si la politique n'est pas respectée dans un compartiment, les CloudFront demandes acheminées vers ce compartiment seront refusées.

Option 1 : accorder l'accès uniquement à CloudFront

Ajoutez une politique de compartiment à chaque compartiment S3 qui permet au principal CloudFront de service d'accéder au compartiment. Utilisez cette option lorsque vous devez également autoriser l'accès direct au bucket depuis d'autres sources.

Example Politique de compartiment S3 pour un compartiment sous-jacent

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontOACAccessViaMRAP",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-us-east-1/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront distribution ID"
                }
            }
        }
    ]
}
```

Option 2 : déléguer l'accès complet au bucket au point Multi-Region d'accès

Accordez Multi-Region au point d'accès un accès complet à chaque compartiment sous-jacent. Avec cette approche, tous les accès au bucket sont contrôlés par la politique des points Multi-

Region d'accès, ce qui simplifie la gestion des accès. Nous recommandons cette option pour les cas d'utilisation ne nécessitant pas d'accès direct au bucket.

Example Politique de compartiment S3 qui délègue l'accès au point Multi-Region d'accès

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DelegateAccessToMRAP",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket-us-east-1",
                "arn:aws:s3:::amzn-s3-demo-bucket-us-east-1/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:DataAccessPointArn":
 "arn:aws:s3::111122223333:accesspoint/Multi-Region-Access-Point-Alias.mrap"
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez Multi-Region un exemple de politique de point d'accès dans le guide de l'utilisateur d'Amazon Simple Storage Service.

SSE-KMS

Si les objets des compartiments S3 sous-jacents sont chiffrés à l'aide du chiffrement côté serveur avec AWS KMS (SSE-KMS), vous devez vous assurer que la CloudFront distribution est autorisée à utiliser la clé. AWS KMS Étant donné que les points Multi-Region d'accès S3 peuvent acheminer des demandes vers des compartiments de plusieurs régions, vous devez ajouter une instruction à la politique de clé KMS dans chaque région utilisée SSE-KMS par un compartiment sous-jacent. Pour plus d'informations sur la modification d'une stratégie de clé, consultez Modification d'une stratégie de clé dans le Guide du développeur AWS Key Management Service .

Example Déclaration de stratégie de clé KMS

L'exemple suivant montre une déclaration de politique de clé KMS qui permet à la CloudFront distribution avec OAC d'accéder à une clé KMS pour SSE-KMS.

```
{
    "Sid": "AllowCloudFrontServicePrincipalSSE-KMS",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudfront.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudfront::111122223333:distribution/CloudFront
 distribution ID"
        }
    }
}
```

> **Important**
>
> Vous devez ajouter cette déclaration de politique de clé à la clé KMS dans chaque région où un compartiment S3 sous-jacent utilise SSE-KMS le chiffrement.

Création du contrôle d’accès d’origine

Pour créer un contrôle d'accès à l'origine (OAC), vous pouvez utiliser le Console de gestion AWS CloudFormation, AWS CLI, ou l' CloudFront API.

> **Note**
>
> Les déclencheurs d'origine Lambda @Edge (demande d'origine et réponse d'origine) sont incompatibles avec les origines qui utilisent un OAC SigV4a, que l'origine soit accessible directement ou via un groupe d'origine.

Console

Pour créer un contrôle d’accès à l’origine

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Accès à l'origine.
3. Choisissez Créer un paramètre de contrôle.
4. Sur l'écran Créer un paramètre de contrôle, procédez comme suit :
   a. Dans le volet Détails, entrez un Nom et (éventuellement) une Description pour le contrôle d'accès à l'origine.
   b. Dans le volet Paramètres, nous vous recommandons de conserver le paramètre par défaut (Signer les demandes (recommandé)). Pour plus d’informations, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine”.
5. Choisissez S3 dans la liste déroulante Type d'origine et sélectionnez l'option Utiliser le protocole de signature SigV4a.
6. Cliquez sur Créer.

   Après avoir créé l'OAC, prenez note de Nom. Vous en aurez besoin au cours de la procédure suivante.

Pour ajouter un contrôle d'accès d'origine à l'origine d'un point d' Multi-Region accès S3 dans une distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez une distribution avec une origine de point d' Multi-Region accès S3 à laquelle vous souhaitez ajouter l'OAC, puis choisissez l'onglet Origins.

3. Sélectionnez l'origine du point d' Multi-Region accès S3 à laquelle vous souhaitez ajouter l'OAC, puis choisissez Modifier.
4. Pour Accès d’origine, sélectionnez Paramètres de contrôle d’accès d’origine (recommandé).
5. Dans le menu déroulant Origin access control (Contrôle d'accès d'origine), choisissez l'OAC que vous souhaitez utiliser.
6. Cliquez sur Enregistrer les modifications.

La distribution commence à se déployer sur tous les emplacements CloudFront périphériques. Lorsqu'un emplacement périphérique reçoit la nouvelle configuration, il signe toutes les demandes qu'il envoie à l'origine du point d' Multi-Region accès S3.

CLI

Utilisez la commande create-origin-access-control :

```
aws cloudfront create-origin-access-control \
    --origin-access-control-config '{
        "Name": "my-s3-mrap-oac",
        "Description": "OAC for S3 Multi-Region Access Point",
        "SigningProtocol": "sigv4a",
        "SigningBehavior": "always",
        "OriginAccessControlOriginType": "s3"
    }'
```

CloudFormation

Spécifiez les valeurs suivantes dans `OriginAccessControlConfig` :

- `SigningProtocol`: `sigv4a`
- `SigningBehavior`:`always`,`never`, ou `no-override`
- `OriginAccessControlOriginType`: `s3`

Example CloudFormation modèle

```
Type: AWS::CloudFront::OriginAccessControl
Properties:
  OriginAccessControlConfig:
    Description: An optional description for the origin access control
```

```
    Name: my-s3-mrap-oac
    OriginAccessControlOriginType: s3
    SigningBehavior: always
    SigningProtocol: sigv4a
```

Comportement de signature

Les options de comportement de signature pour les origines des points d' Multi-Region accès S3 sont les mêmes que celles pour les origines des compartiments Amazon S3 classiques. Pour plus d'informations, consultez the section called “Paramètres avancés pour le contrôle d'accès à l'origine” la section Restreindre l'accès à une origine Amazon S3.

Restriction de l’accès aux Application Load Balancers

Vous pouvez utiliser des équilibreurs de charge d'applications internes et connectés à Internet avec Amazon. CloudFront Vous pouvez utiliser des équilibreurs de charge d'application internes dans des sous-réseaux privés CloudFront en utilisant VPC Origins. CloudFront Les origines VPC vous permettent de diffuser du contenu à partir d'applications hébergées dans des sous-réseaux VPC privés sans les exposer à l'Internet public. Pour de plus amples informations, veuillez consulter Restriction de l’accès avec les origines de VPC.

Si vous utilisez un équilibreur de charge d'application connecté à Internet avec CloudFront, vous pouvez utiliser les mesures de sécurité suivantes pour empêcher les utilisateurs d'accéder directement à un équilibreur de charge d'application et autoriser l'accès uniquement via. CloudFront

1. Configurez CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes qu'il envoie à l'équilibreur de charge des applications.
2. Configurez l'Application Load Balancer pour transférer uniquement les demandes contenant l'en-tête HTTP personnalisé.
3. Exigez l’utilisation de HTTPS pour renforcer la sécurité de cette solution.

CloudFront peut également contribuer à réduire la latence et même à absorber certaines attaques par déni de service distribué (DDoS).

Si votre cas d'utilisation nécessite un double accès aux applications Web à la fois depuis Application Load Balancer CloudFront et directement via Internet, envisagez de diviser les API de vos applications Web comme suit :

- Des API qui doivent passer CloudFront. Dans ce cas, envisagez d'utiliser un Application Load Balancer privé distinct comme origine.
- API nécessitant un accès via Application Load Balancer. Dans ce cas, vous contournez CloudFront.

Sinon, pour une application Web ou un autre contenu diffusé par un équilibreur de charge d'application connecté à Internet dans Elastic Load Balancing, CloudFront vous pouvez mettre en cache des objets et les diffuser directement aux utilisateurs (spectateurs), réduisant ainsi la charge de votre équilibreur de charge d'application. Un équilibreur de charge accessible sur Internet possède un nom DNS publiquement résolu et achemine les demandes des clients vers les cibles via Internet.

Pour plus d'informations, consultez les rubriques suivantes. Une fois ces étapes terminées, les utilisateurs ne peuvent accéder à votre équilibreur de charge d'application que via CloudFront.

Rubriques

- Configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes
- Configuration d'un Application Load Balancer pour transférer uniquement les demandes contenant un en-tête spécifique
- (Facultatif) Améliorer la sécurité de cette solution
- (Facultatif) Limitez l'accès à l'origine en utilisant AWS-liste de préfixes gérée pour CloudFront

Configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes

Vous pouvez configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes qu'il envoie à votre origine (dans ce cas, un équilibreur de charge d'application).

> **Important**
>
> Ce cas d'utilisation repose sur le fait de garder secrets le nom et la valeur de l'en-tête personnalisé. Si le nom et la valeur d'en-tête ne sont pas secrets, d'autres clients HTTP peuvent potentiellement les inclure dans les demandes qu'ils envoient directement à l'Application Load Balancer. Cela peut entraîner le comportement de l'équilibreur de charge des applications comme si les demandes provenaient d' CloudFront un autre endroit. Pour éviter cela, gardez le nom et la valeur de l'en-tête personnalisé secrets.

Vous pouvez configurer CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes d'origine à l'aide de la CloudFront console ou de l' CloudFront API. CloudFormation

Pour ajouter un en-tête HTTP personnalisé (CloudFront console)

Dans la CloudFront console, utilisez le paramètre Origin Custom Headers dans Origin Settings. Entrez le Nom de l'en-tête et sa Valeur.

> **Note**
>
> En production, utilisez des noms et des valeurs d'en-têtes générés aléatoirement. Traitez les noms et les valeurs d'en-tête en tant qu'informations d'identification sécurisées, comme les noms d'utilisateur et les mots de passe.

Vous pouvez modifier le paramètre Origin Custom Headers lorsque vous créez ou modifiez l'origine d'une CloudFront distribution existante et lorsque vous créez une nouvelle distribution. Pour plus d'informations, consultez Mettre à jour une distribution et Créer une distribution.

Pour ajouter un en-tête HTTP personnalisé (CloudFormation)

Dans un CloudFormation modèle, utilisez la `OriginCustomHeaders` propriété, comme illustré dans l'exemple suivant.

> **Note**
>
> Le nom et la valeur de l'en-tête dans cet exemple n'existent qu'à des fins de démonstration. En production, utilisez des valeurs générées aléatoirement. Traitez le nom et la valeur de l'en-tête en tant qu'informations d'identification sécurisées, comme un nom d'utilisateur et un mot de passe.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestDistribution:
    Type: 'AWS::CloudFront::Distribution'
    Properties:
      DistributionConfig:
        Origins:
          - DomainName: app-load-balancer.example.com
```

```
            Id: Example-ALB
            CustomOriginConfig:
              OriginProtocolPolicy: https-only
              OriginSSLProtocols:
                - TLSv1.2
            OriginCustomHeaders:
               - HeaderName: X-Custom-Header
                 HeaderValue: random-value-1234567890
        Enabled: 'true'
        DefaultCacheBehavior:
          TargetOriginId: Example-ALB
          ViewerProtocolPolicy: allow-all
          CachePolicyId: 658327ea-f89d-4fab-a63d-7e88639e58f6
        PriceClass: PriceClass_All
        ViewerCertificate:
          CloudFrontDefaultCertificate: 'true'
```

Pour plus d'informations, consultez l'origine et les OriginCustomHeader propriétés dans le Guide de AWS CloudFormation l'utilisateur.

Pour ajouter un en-tête HTTP personnalisé (CloudFront API)

Dans l' CloudFront API, utilisez l'`CustomHeaders`objet qu'il contient`Origin`. Pour plus d'informations, consultez CreateDistribution et consultez UpdateDistribution l'Amazon CloudFront API Reference, ainsi que la documentation de votre SDK ou de tout autre client d'API.

Il existe certains noms d'en-tête que vous ne pouvez pas spécifier en tant qu'en-têtes personnalisés d'origine. Pour de plus amples informations, veuillez consulter En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine.

Configuration d’un Application Load Balancer pour transférer uniquement les demandes contenant un en-tête spécifique

Après avoir configuré CloudFront pour ajouter un en-tête HTTP personnalisé aux requêtes qu'il envoie à votre équilibreur de charge d'applications (voir la section précédente), vous pouvez configurer l'équilibreur de charge pour ne transmettre que les demandes contenant cet en-tête personnalisé. Pour ce faire, ajoutez une nouvelle règle et modifiez la règle par défaut dans l’écouteur de votre équilibreur de charge.

Conditions préalables

Pour utiliser les procédures suivantes, vous avez besoin d'un Application Load Balancer avec au moins un écouteur. Si vous n'en avez pas encore créé, reportez-vous à la section Créer un Application Load Balancer dans le guide de l'utilisateur pour les Application Load Balancers.

Les procédures suivantes modifient un écouteur HTTPS. Vous pouvez utiliser le même processus pour modifier un écouteur HTTP.

Pour mettre à jour les règles dans un écouteur d'Application Load Balancer

1. Ajoutez une nouvelle règle. Suivez les instructions indiquées dans Ajouter une règle, avec les modifications suivantes :
   - Ajoutez la règle à l'équilibreur de charge qui est à l'origine de votre CloudFront distribution.
   - Pour Ajouter une condition, choisissez En-tête HTTP. Spécifiez le nom et la valeur de l'en-tête HTTP que vous avez ajoutés en tant qu'en-tête personnalisé d'origine dans CloudFront.
   - Pour Ajouter une action, choisissez Transférer vers. Choisissez le groupe cible dans lequel vous souhaitez transférer les demandes.
2. Modifiez la règle par défaut dans l'écouteur de votre équilibreur de charge. Suivez les instructions indiquées dans Modifier une règle, avec les modifications suivantes :
   - Modifiez la règle par défaut de l'équilibreur de charge qui est à l'origine de votre CloudFront distribution.
   - Supprimez l'action par défaut, puis pour Ajouter une action, choisissez Renvoyer une réponse fixe.
   - Pour le Code de réponse, saisissez **`403`**.
   - Pour Corps de réponse, saisissez **`Access denied`**.

Après avoir terminé ces étapes, votre écouteur d'équilibreur de charge dispose de deux règles. Une règle transmet les requêtes contenant l'en-tête HTTP (requêtes provenant de CloudFront). L'autre règle envoie une réponse fixe à toutes les autres demandes (demandes qui ne proviennent pas de CloudFront).

Vous pouvez vérifier que la solution fonctionne en envoyant une demande à votre CloudFront distribution et une autre à votre équilibreur de charge d'application. La demande de CloudFront renvoi de votre application Web ou de votre contenu, et celle envoyée directement à votre Application Load Balancer renvoie une `403` réponse sous forme de message `Access denied` en texte brut.

(Facultatif) Améliorer la sécurité de cette solution

Pour améliorer la sécurité de cette solution, vous pouvez configurer votre CloudFront distribution pour qu'elle utilise toujours le protocole HTTPS lors de l'envoi de requêtes à votre équilibreur de charge d'application. N'oubliez pas que cette solution ne fonctionne que si vous gardez le nom et la valeur de l'en-tête personnalisé secrètes. L'utilisation de HTTPS peut aider à empêcher un compte-écoute de découvrir le nom et la valeur de l'en-tête. Nous vous recommandons également de faire changer périodiquement le nom et la valeur de l'en-tête.

Utiliser HTTPS pour les demandes d'origine

CloudFront Pour configurer l'utilisation du protocole HTTPS pour les demandes d'origine, définissez le paramètre Politique de protocole d'origine sur HTTPS uniquement. Ce paramètre est disponible dans la CloudFront console et dans l' CloudFront API. CloudFormation Pour de plus amples informations, veuillez consulter Protocole (origines personnalisées uniquement).

Ce qui suit s'applique également lorsque vous configurez CloudFront pour utiliser le protocole HTTPS pour les demandes d'origine :

- Vous devez configurer CloudFront pour transmettre l'`Host`en-tête à l'origine avec la politique de demande d'origine. Vous pouvez utiliser la politique de AllViewer gestion des demandes d'origine.
- Assurez-vous que votre Application Load Balancer dispose d'un écouteur HTTPS (comme indiqué dans la section précédente). Pour plus d'informations, consultez la section Création d'un écouteur HTTPS dans le guide de l'utilisateur pour les Application Load Balancers. L'utilisation d'un écouteur HTTPS nécessite que vous disposiez d'un SSL/TLS certificat correspondant au nom de domaine qui est acheminé vers votre équilibreur de charge d'application.
- SSL/TLS les certificats pour ne CloudFront peuvent être demandés (ou importés) que `us-east-1` Région AWS dans l'entrée AWS Certificate Manager (ACM). Comme il CloudFront s'agit d'un service mondial, il distribue automatiquement le certificat de la `us-east-1` région à toutes les régions associées à votre CloudFront distribution.
  - Par exemple, si vous disposez d'un équilibreur de charge d'application (ALB) dans la `ap-southeast-2` région, vous devez configurer les SSL/TLS certificats à la fois dans la `ap-southeast-2` région (pour utiliser le protocole HTTPS entre CloudFront et l'origine ALB) et dans la `us-east-1` région (pour utiliser le protocole HTTPS entre les utilisateurs et). CloudFront Les deux certificats doivent correspondre au nom de domaine qui est acheminé vers votre Application Load Balancer. Pour de plus amples informations, veuillez consulter Région AWS for AWS Certificate Manager.

- Si les utilisateurs finaux (également appelés spectateurs ou clients) de votre application Web peuvent utiliser HTTPS, vous pouvez également configurer CloudFront pour préférer (voire exiger) des connexions HTTPS de la part des utilisateurs finaux. Pour ce faire, utilisez le paramètre Stratégie de protocole d'utilisateur. Vous pouvez le définir pour rediriger les utilisateurs finaux de HTTP vers HTTPS ou pour rejeter les demandes utilisant HTTP. Ce paramètre est disponible dans la CloudFront console et dans l' CloudFront API. CloudFormation Pour de plus amples informations, veuillez consulter Viewer Protocol Policy.

Changer le nom et la valeur de l'en-tête

En plus d'utiliser HTTPS, nous vous recommandons également de changer périodiquement le nom et la valeur de l'en-tête. Les étapes de haut niveau pour ce faire sont les suivantes :

1. Configurez CloudFront pour ajouter un en-tête HTTP personnalisé supplémentaire aux requêtes qu'il envoie à l'équilibreur de charge des applications.
2. Mettez à jour la règle de l’écouteur de l'Application Load Balancer pour transférer les demandes contenant cet en-tête HTTP personnalisé supplémentaire.
3. Configurez CloudFront pour arrêter d'ajouter l'en-tête HTTP personnalisé d'origine aux requêtes qu'il envoie à l'équilibreur de charge des applications.
4. Mettez à jour la règle de l'écouteur de l'Application Load Balancer pour arrêter le transfert des demandes contenant l'en-tête HTTP personnalisé d'origine.

Pour plus d'informations sur la réalisation de ces étapes, consultez les sections précédentes.

(Facultatif) Limitez l'accès à l'origine en utilisant AWS-liste de préfixes gérée pour CloudFront

Pour restreindre davantage l'accès à votre équilibreur de charge d'application, vous pouvez configurer le groupe de sécurité associé à l'équilibreur de charge d'application afin qu'il n'accepte que le trafic provenant du CloudFront moment où le service utilise une liste de AWS préfixes gérée. Cela empêche le trafic qui ne CloudFront provient pas d'atteindre votre équilibreur de charge d'application au niveau de la couche réseau (couche 3) ou de la couche transport (couche 4).

Pour plus d'informations, consultez l'article de CloudFront blog Amazon intitulé Limiter l'accès à vos origines à l'aide de la liste de préfixes AWS-managed.

Restriction de la distribution géographique de votre contenu

Vous pouvez utiliser des restrictions géographiques, parfois appelées blocage géographique, pour empêcher les utilisateurs situés dans des zones géographiques spécifiques d'accéder au contenu que vous distribuez via une CloudFront distribution Amazon. Pour utiliser les restrictions géographiques, vous avez deux options :

- Utilisez la fonction de restrictions CloudFront géographiques. Choisissez cette option pour limiter l’accès à tous les fichiers associés à une distribution et pour limiter l’accès au niveau du pays.
- Utiliser un service de géolocalisation tiers. Utilisez cette option pour limiter l’accès à un sous-ensemble des fichiers associés à une distribution ou pour le limiter à un niveau de détail plus fin que le niveau pays.

Rubriques

- Utiliser des restrictions CloudFront géographiques
- Utilisation d’un service de géolocalisation tiers

Utiliser des restrictions CloudFront géographiques

Lorsqu'un utilisateur demande votre contenu, il diffuse CloudFront généralement le contenu demandé, quel que soit l'endroit où se trouve l'utilisateur. Si vous devez empêcher les utilisateurs de certains pays d'accéder à votre contenu, vous pouvez utiliser la fonction de restrictions CloudFront géographiques pour effectuer l'une des opérations suivantes :

- Accorder à vos utilisateurs l’autorisation d’accéder à votre contenu seulement s’ils résident dans un des pays figurant dans la liste des pays autorisés.
- Empêcher vos utilisateurs d’accéder à votre contenu s’ils résident dans un des pays interdits de la liste d’exclusion.

Par exemple, si une demande provient d'un pays où vous n'êtes pas autorisé à diffuser votre contenu, vous pouvez utiliser des restrictions CloudFront géographiques pour bloquer la demande.

> **Note**
>
> CloudFront détermine la localisation de vos utilisateurs à l'aide d'une base de données tierce. La précision de la correspondance entre les adresses IP et les pays varie selon la région.

Selon des tests récents, la précision globale est de 99,8 %. S'il n'est pas CloudFront possible de déterminer la position d'un utilisateur, CloudFront diffuse le contenu que l'utilisateur a demandé.

Les restrictions géographiques fonctionnent comme suit :

1. Imaginons que vous n'ayez le droit de distribuer votre contenu qu'au Liechtenstein. Vous mettez à jour votre CloudFront distribution pour ajouter une liste d'autorisations contenant uniquement le Liechtenstein. (Vous pouvez, à la place, ajouter une liste d'exclusion contenant tous les pays, à l'exception du Liechtenstein.)
2. Un utilisateur de Monaco demande votre contenu et le DNS achemine la demande vers un emplacement CloudFront périphérique à Milan, en Italie.
3. L'emplacement périphérique de Milan recherche votre distribution et détermine que l'utilisateur de Monaco n'a pas l'autorisation de télécharger votre contenu.
4. CloudFront renvoie un code d'état HTTP `403 (Forbidden)` à l'utilisateur.

Note

Les restrictions géographiques ne s'appliquent pas aux demandes de validation de certificats pour les certificats CloudFront gérés. Lorsque vous utilisez un certificat CloudFront géré, les demandes adressées au `/.well-known/pki-validation/` chemin sont exclues des règles de restriction géographique. Cela garantit que les autorités de certification peuvent valider votre certificat à partir des multiples points de vue du réseau géographiquement distribué requis pour l'émission et le renouvellement, quelle que soit votre configuration de restriction géographique.

Si vous l'utilisez AWS WAF avec votre distribution, assurez-vous que vos AWS WAF règles (y compris les règles de contrôle des robots) ne bloquent pas les requêtes vers le `/.well-known/pki-validation/` chemin. Le blocage de ces demandes peut empêcher la validation du certificat de se terminer correctement.

Vous pouvez éventuellement configurer CloudFront pour renvoyer un message d'erreur personnalisé à l'utilisateur, et vous pouvez spécifier la durée pendant laquelle vous souhaitez CloudFront mettre en cache la réponse d'erreur pour le fichier demandé. La valeur par défaut est de 10 secondes. Pour

plus d'informations, consultez Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques.

Les restrictions géographiques s'appliquent à la totalité d'une distribution. Si vous devez appliquer une restriction à une partie de votre contenu et une autre restriction (ou aucune restriction) à une autre partie de votre contenu, vous devez créer des CloudFront distributions distinctes ou utiliser un service de géolocalisation tiers.

Si vous activez les journaux CloudFront standard (journaux d'accès), vous pouvez identifier les demandes CloudFront rejetées en recherchant les entrées de journal contenant la valeur de `sc-status` (le code d'état HTTP)`403`. Toutefois, en utilisant uniquement les journaux standard, vous ne pouvez pas distinguer une demande CloudFront rejetée en fonction de la localisation de l'utilisateur d'une demande CloudFront rejetée parce que l'utilisateur n'était pas autorisé à accéder au fichier pour une autre raison. Si vous disposez d'un service de géolocalisation tiers tel que Digital Element ou MaxMind, vous pouvez identifier l'emplacement des demandes en fonction de l'adresse IP figurant dans la colonne `c-ip` (IP du client) des journaux d'accès. Pour plus d'informations sur les journaux CloudFront standard, consultezJournaux d'accès (journaux standard).

La procédure suivante explique comment utiliser la CloudFront console pour ajouter des restrictions géographiques à une distribution existante. Pour plus d'informations sur l'utilisation de la console pour créer une distribution, consultez Créer une distribution.

Pour ajouter des restrictions géographiques à votre distribution CloudFront Web (console)

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Distributions, puis choisissez la distribution que vous souhaitez mettre à jour.
3. Choisissez l'onglet Sécurité, puis sélectionnez Restrictions géographiques.
4. Choisissez Modifier.
5. Sélectionnez Allow list (Liste verte) pour créer une liste des pays autorisés, ou Liste rouge pour créer une liste des pays interdits.
6. Ajoutez les pays souhaités à la liste, puis choisissez Save changes (Enregistrer les modifications).

Utilisation d’un service de géolocalisation tiers

Grâce à la fonction de restrictions CloudFront géographiques, vous contrôlez la distribution de votre contenu au niveau du pays pour tous les fichiers que vous distribuez via une distribution Web donnée. Si vous avez un cas d'utilisation de restrictions géographiques qui ne suivent pas les frontières des pays, ou si vous souhaitez restreindre l'accès à certains des fichiers que vous diffusez par une distribution donnée, vous pouvez les CloudFront associer à un service de géolocalisation tiers. Vous pouvez ainsi contrôler l’accès à votre contenu en fonction non seulement du pays, mais aussi de la ville ou du code postal, voire de la latitude et de la longitude.

Lorsque vous utilisez un service de géolocalisation tiers, nous vous recommandons d'utiliser des URL CloudFront signées, avec lesquelles vous pouvez spécifier une date et une heure d'expiration après lesquelles l'URL n'est plus valide. En outre, nous vous recommandons d'utiliser un compartiment Amazon S3 comme origine, car vous pouvez ensuite utiliser un contrôle CloudFront d'accès à l'origine pour empêcher les utilisateurs d'accéder à votre contenu directement depuis l'origine. Pour plus d’informations sur les URL signées et les contrôles d’accès à l’origine, consultez Offre de contenu privé avec des URL et des cookies signés.

Les étapes ci-après expliquent comment contrôler l’accès à vos fichiers à l’aide d’un service de géolocalisation tiers.

Pour utiliser un service de géolocalisation tiers afin de restreindre l'accès aux fichiers d'une distribution CloudFront

1. Obtenez un compte avec un service de géolocalisation.
2. Chargez votre contenu sur un compartiment Amazon S3.
3. Configurez Amazon CloudFront et Amazon S3 pour diffuser du contenu privé. Pour plus d’informations, consultez Offre de contenu privé avec des URL et des cookies signés.
4. Ecrivez votre application web pour exécuter ce qui suit :

   - Envoyez l’adresse IP de chaque demande utilisateur au service de géolocalisation.
   - Évaluez la valeur renvoyée par le service de géolocalisation pour déterminer si l'utilisateur se trouve à l'endroit où vous souhaitez CloudFront diffuser votre contenu.
   - Si vous souhaitez diffuser votre contenu là où se trouve l'utilisateur, générez une URL signée pour votre CloudFront contenu. Si vous ne souhaitez pas distribuer de contenu à cet emplacement, renvoyez le code d'état HTTP `403 (Forbidden)` à l'utilisateur. Vous pouvez également configurer CloudFront pour renvoyer un message d'erreur personnalisé. Pour plus

d'informations, consultez the section called "Création d'une page d'erreur personnalisée pour des codes d'état HTTP spécifiques".

Pour plus d'informations, consultez la documentation du service de géolocalisation que vous utilisez.

Vous pouvez utiliser une variable de serveur web pour obtenir les adresses IP des utilisateurs qui visitent votre site web. Notez les avertissements suivants :

- Si votre serveur web n'est pas connecté à Internet via un équilibreur de charge, vous pouvez utiliser une variable de serveur web pour obtenir l'adresse IP distante. Toutefois, cette adresse IP n'est pas toujours l'adresse IP de l'utilisateur. Il peut également s'agir de l'adresse IP d'un serveur proxy, selon la façon dont l'utilisateur est connecté à Internet.
- Si votre serveur web est connecté à Internet via un équilibreur de charge, une variable de serveur web peut contenir l'adresse IP de l'équilibreur de charge, et non celle de l'utilisateur. Dans cette configuration, nous vous recommandons d'utiliser la dernière adresse IP de l'en-tête HTTP `X-Forwarded-For`. Cet en-tête contient généralement plusieurs adresses IP, la plupart concernant des proxys ou des équilibreurs de charge. La dernière adresse IP de la liste est celle qui est très vraisemblablement associée à l'emplacement géographique de l'utilisateur.

Si votre serveur web n'est pas connecté à un équilibreur de charge, nous vous recommandons d'utiliser les variables de serveur web à la place de l'en-tête `X-Forwarded-For` pour éviter l'usurpation d'adresse IP.

Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles

Avec Amazon CloudFront, vous pouvez appliquer des connexions sécurisées de bout en bout aux serveurs d'origine à l'aide du protocole HTTPS. Field-level le chiffrement ajoute une couche de sécurité supplémentaire que vous pouvez utiliser pour protéger des données spécifiques tout au long du traitement du système afin que seules certaines applications puissent les voir.

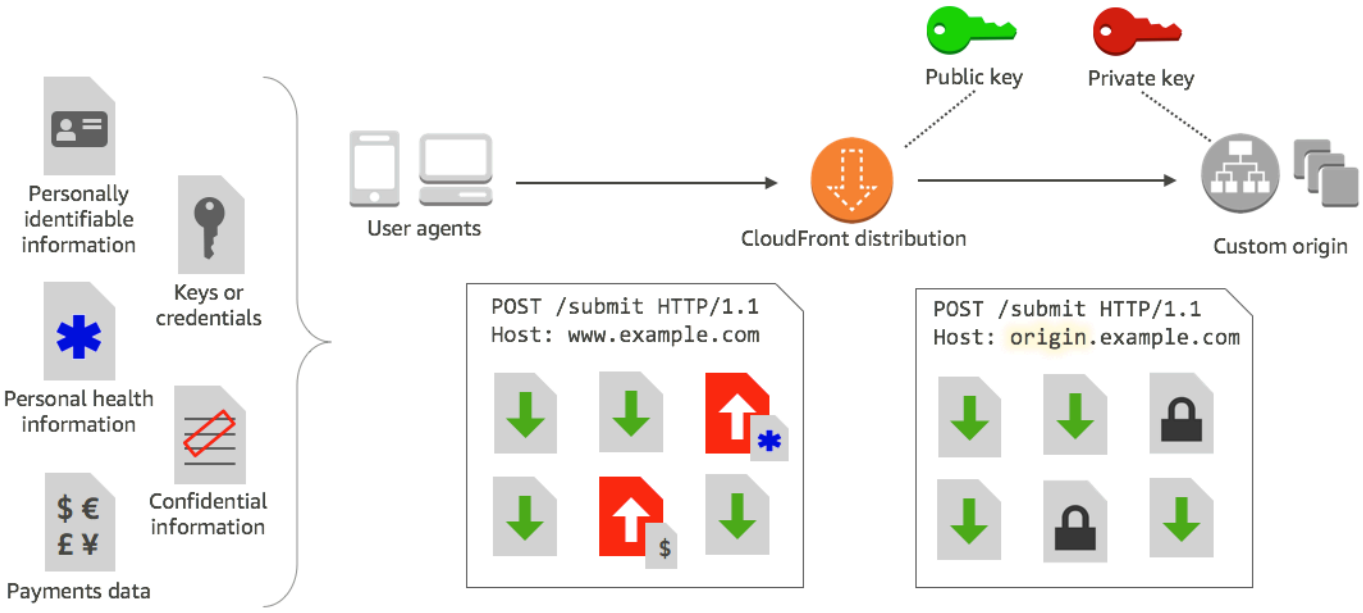
Grâce au chiffrement au niveau des champs, vous pouvez permettre à vos utilisateurs de télécharger en toute sécurité des informations sensibles sur vos serveurs Web. Les informations sensibles fournies par vos utilisateurs sont chiffrées à la périphérie, à proximité de l'utilisateur, et restent chiffrées tout le long de votre pile d'applications. Ce chiffrement garantit que seules les applications

qui ont besoin des données et qui disposent des informations d'identification nécessaires pour les déchiffrer peuvent le faire.

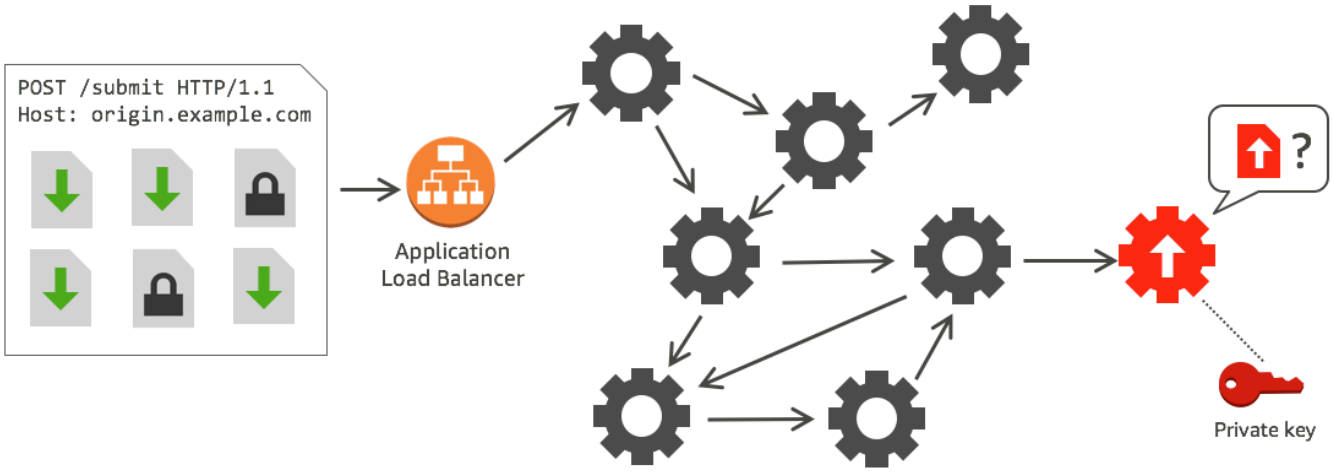
Pour utiliser le chiffrement au niveau des champs, lorsque vous configurez votre CloudFront distribution, spécifiez l'ensemble de champs des requêtes POST que vous souhaitez chiffrer, ainsi que la clé publique à utiliser pour les chiffrer. Vous pouvez chiffrer jusqu'à 10 champs de données dans une requête. (Vous ne pouvez pas chiffrer toutes les données dans une requête avec chiffrement au niveau du champ ; vous devez spécifier des champs individuels à chiffrer).

Lorsque la requête HTTPS avec chiffrement au niveau du champ est réacheminée vers l'origine, et que la requête est acheminée dans votre application ou sous-système d'origine, les données sensibles sont toujours chiffrées, ce qui réduit le risque de violation ou de perte accidentelle des données sensibles. Les composants devant accéder aux données sensibles pour des raisons professionnelles, comme un système de traitement de paiement qui aurait besoin d'accéder à un numéro de crédit, peuvent utiliser la clé privée adéquate pour déchiffrer les données et y accéder.

> **Note**
>
> Pour utiliser le chiffrement au niveau du champ, votre origine doit prendre en charge l'encodage segmenté.



CloudFront le chiffrement au niveau des champs utilise un chiffrement asymétrique, également appelé chiffrement à clé publique. Vous fournissez une clé publique à CloudFront, et toutes les données sensibles que vous spécifiez sont automatiquement cryptées. La clé que vous fournissez CloudFront ne peut pas être utilisée pour déchiffrer les valeurs chiffrées ; seule votre clé privée peut le faire.



Rubriques

- Présentation du chiffrement au niveau du champ
- Configuration du chiffrement au niveau du champ
- Déchiffrage de champs de données à votre origine

Présentation du chiffrement au niveau du champ

Les étapes suivantes présentent la configuration de chiffrement au niveau du champ. Pour connaître les étapes spécifiques, consultez Configuration du chiffrement au niveau du champ.

1. Obtenez une paire de clés publique/clé privée. Vous devez obtenir et ajouter la clé publique avant de commencer à configurer le chiffrement au niveau du champ dans CloudFront
2. Créez un profil de chiffrement au niveau du champ. Field-level les profils de chiffrement, dans lesquels vous créez CloudFront, définissent les champs que vous souhaitez chiffrer.
3. Créez une configuration de chiffrement au niveau du champ. Une configuration spécifie les profils à utiliser selon le type de contenu de la requête ou un argument de requête pour chiffrer des champs de données spécifiques. Vous pouvez également choisir les options de

comportement de transfert de demande que vous souhaitées pour différents scénarios. Par exemple, vous pouvez définir le comportement lorsque le nom de profil spécifié par l'argument de requête dans une URL de demande n'existe pas dans CloudFront.

4. Lien vers un comportement de cache. Associez la configuration à un comportement de cache pour une distribution, pour spécifier quand CloudFront doit chiffrer des données.

Configuration du chiffrement au niveau du champ

Suivez ces étapes pour commencer à utiliser le chiffrement au niveau du champ. Pour en savoir plus sur les quotas (auparavant appelés limites) liés au chiffrement au niveau du champ, consultez Quotas.

- Étape 1 : créer une paire de clés RSA
- Étape 2 : ajoutez votre clé publique à CloudFront
- Étape 3 : créer un profil de chiffrement au niveau du champ
- Étape 4 : créer une configuration
- Étape 5 : ajouter une configuration à un comportement de cache

Étape 1 : créer une paire de clés RSA

Pour commencer, vous devez créer une paire de clés RSA qui inclut une clé publique et une clé privée. La clé publique permet CloudFront de chiffrer les données et la clé privée permet aux composants de votre origine de déchiffrer les champs qui ont été chiffrés. Vous pouvez utiliser OpenSSL ou un autre outil pour créer une paire de clés. La taille de la clé doit être de 2 048 bits.

Par exemple, si vous utilisez OpenSSL, vous pouvez exécuter la commande suivante pour générer une paire de clés avec une longueur de 2048 bits et l'enregistrer dans le fichier `private_key.pem`:

```
openssl genrsa -out private_key.pem 2048
```

Le fichier obtenu contient à la fois la clé publique et la clé privée. Pour extraire la clé publique de ce fichier, exécutez la commande suivante :

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

Le fichier de clé publique (`public_key.pem`) contient la valeur de clé codée que vous collez à l'étape suivante.

Étape 2 : ajoutez votre clé publique à CloudFront

Une fois que vous avez obtenu votre paire de clés RSA, ajoutez-la à CloudFront.

Pour ajouter votre clé publique à CloudFront (console)

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, sélectionnez Clé publique.
3. Choisissez Ajouter une clé publique.
4. Dans Nom de clé, tapez un nom unique pour la clé. Le nom ne peut pas contenir d'espaces et ne peut contenir que des caractères alphanumériques, des traits de soulignement (_) et des tirets (-). Le nombre maximum de caractères est 128.
5. Pour Key value (Valeur de clé), collez la valeur de clé encodée pour votre clé publique, y compris les lignes `-----BEGIN PUBLIC KEY-----` et `-----END PUBLIC KEY-----`.
6. Pour Commentaire, ajoutez un commentaire facultatif. Par exemple, vous pouvez inclure la date d'expiration pour la clé publique.
7. Choisissez Ajouter.

Vous pouvez ajouter d'autres touches à utiliser CloudFront en répétant les étapes de la procédure.

Étape 3 : créer un profil de chiffrement au niveau du champ

Après avoir ajouté au moins une clé publique à CloudFront, créez un profil CloudFront indiquant les champs à chiffrer.

Créer un profil de chiffrement au niveau du champ (console)

1. Dans le volet de navigation, choisissez Field-level le chiffrement.
2. Choisissez Créer un profil.
3. Remplissez les champs suivants :

   Profile name (Nom du profil)

   Saisissez un nom unique pour le profil. Le nom ne peut pas contenir d'espaces et ne peut contenir que des caractères alphanumériques, des traits de soulignement (_) et des tirets (-). Le nombre maximum de caractères est 128.

Nom de clé publique

Dans la liste déroulante, choisissez le nom de la clé publique que vous avez ajoutée CloudFront à l'étape 2. CloudFront utilise la clé pour chiffrer les champs que vous spécifiez dans ce profil.

Nom du fournisseur

Saisissez une phrase facilitant l'identification de la clé, comme le fournisseur de la paire de clés. Ces informations, tout comme la clé privée, sont nécessaires lors du déchiffrement des champs de données par les applications. Le nom du fournisseur ne peut pas contenir d'espaces et ne peut contenir que des caractères alphanumériques, des deux-points (:), des traits de soulignement (_) et des tirets (-). Le nombre maximum de caractères est 128.

Modèle de nom de champ

Saisissez les noms des champs de données, ou des modèles identifiant des noms de champs de données dans la requête, que vous voulez que CloudFront chiffre. Sélectionnez l'option + pour ajouter tous les champs que vous souhaitez chiffrer avec cette clé.

Pour le modèle de nom de champ, vous pouvez taper le nom complet du champ de données DateOfBirth, par exemple, ou simplement la première partie du nom avec un caractère générique (*), comme CreditCard *. Le modèle de champ de nom ne peut contenir que des caractères alphanumériques, des crochets ([et]), des points (.), des traits de soulignement (_) et des tirets (-) et en option, le métacaractère (*).

N'utilisez pas de caractères qui se chevauchent pour différents modèles de nom de champ. Par exemple, si vous avez un modèle de nom de champ ABC*, vous ne pouvez pas ajouter un autre modèle de nom de champ AB*. De plus, les noms de champ sont sensibles à la casse et le nombre maximum de caractères ne doit pas dépasser 128.

Commentaire

(Facultatif) Saisissez un commentaire sur ce profil. Le nombre maximum de caractères à utiliser est de 128.

4. Une fois les champs remplis, choisissez Créer un profil.
5. Pour ajouter d'autres profils, Sélectionnez Ajouter un profil.

Étape 4 : créer une configuration

Après avoir créé un ou plusieurs profils de chiffrement au niveau des champs, créez une configuration qui spécifie le type de contenu de la demande qui inclut les données à chiffrer, le profil à utiliser pour le chiffrement et d'autres options qui spécifient la manière dont vous CloudFront souhaitez gérer le chiffrement.

Par exemple, lorsque vous ne CloudFront pouvez pas chiffrer les données, vous pouvez spécifier s'il CloudFront faut bloquer ou transmettre une demande à votre origine dans les scénarios suivants :

- Lorsque le type de contenu d'une demande ne figure pas dans une configuration, vous n'avez peut-être pas ajouté de type de contenu à une configuration. Dans ce cas, vous pouvez spécifier si elle CloudFront transmet la demande avec ce type de contenu à l'origine sans chiffrer les champs de données, ou si elle bloque la demande et renvoie une erreur.

  > **Note**
  >
  > Si vous ajoutez un type de contenu à une configuration mais que vous n'avez pas spécifié de profil à utiliser avec ce type, CloudFront transférez toujours les demandes avec ce type de contenu à l'origine.

- Lorsque le nom de profil fourni dans un argument de requête est inconnu — Lorsque vous spécifiez l'argument de `fle-profile` requête avec un nom de profil qui n'existe pas pour votre distribution, vous pouvez spécifier si vous CloudFront devez envoyer la demande à l'origine sans chiffrer les champs de données, ou bloquer la demande et renvoyer une erreur.

Dans une configuration, vous pouvez également spécifier si fournir un profil en tant qu'argument de requête dans une URL substitue un profil que vous avez mappé vers le type de contenu de cette requête. Par défaut, CloudFront utilise le profil que vous avez mappé à un type de contenu, si vous en spécifiez un. Vous pouvez ainsi avoir un profil utilisé par défaut, mais décider d'appliquer un profil différent pour certaines demandes.

Donc, par exemple, vous pouvez spécifier (dans votre configuration) **`SampleProfile`** comme profil d'argument de requête à utiliser. Ensuite, vous pouvez utiliser l'URL à la `https://d1234.cloudfront.net?fle-profile=SampleProfile` place de`https://d1234.cloudfront.net`, à CloudFront utiliser **`SampleProfile`** pour cette demande, au lieu du profil que vous auriez configuré pour le type de contenu de la demande.

Vous pouvez créer jusqu'à 10 configurations pour un seul compte, puis associer l'une des configurations au comportement de cache d'une distribution pour le compte.

Créer une configuration de chiffrement au niveau du champ (console)

1. Sur la page Field-level de chiffrement, choisissez Créer une configuration.

   Remarque : Si vous n'avez pas créé de profil, vous ne verrez pas l'option permettant de créer une configuration.
2. Renseignez les champs suivants pour spécifier le profil à utiliser. (Certains champs ne peuvent être modifiés).

   Type de contenu (non modifiable)

   Le type de contenu est défini comme `application/x-www-form-urlencoded` et ne peut être modifié.

   ID de profil par défaut (facultatif)

   Dans la liste déroulante, sélectionnez le profil que vous souhaitez mapper au type de contenu dans le champ Type de contenu.

   Format de contenu (non modifiable)

   Le format du contenu est défini comme `URLencoded` et ne peut être modifié.
3. Si vous souhaitez modifier le comportement CloudFront par défaut des options suivantes, cochez la case appropriée.

   Réacheminer une requête vers l'origine lorsque le type de contenu de a requête n'est pas configuré

   Sélectionnez la case à cocher pour permettre à la requête d'atteindre votre origine si vous n'avez pas spécifié de profil à utiliser pour le type de contenu de la requête.

   Substituer le profil d'un type de contenu avec un argument de requête fourni

   Sélectionnez la case à cocher pour autoriser un profil fourni dans un argument de requête à substituer le profil que vous avez spécifié pour un type de contenu.
4. Si vous sélectionnez la case à cocher pour autoriser un argument de requête à remplacer le profil par défaut, vous devez renseigner les champs supplémentaires suivants pour la configuration. Vous pouvez créer jusqu'à cinq de ces mappages d'argument de requête à utiliser avec les requêtes.

Argument de requête

Saisissez la valeur que vous voulez inclure dans l'URL pour l'argument de requête de `fle-profile`. Cette valeur indique à CloudFront d'utiliser l'ID de profil (que vous indiquez dans le champ suivant) associée à cet argument de requête de chiffrement au niveau du champ pour cette requête.

Le nombre maximum de caractères à utiliser est de 128. La valeur ne doit pas contenir d'espaces et ne comporter que des caractères alphanumériques ou les caractères suivants : tiret (-), point (.), trait de soulignement (_), astérisque (*), signe plus (+), pourcentage (%).

ID de profil

Dans la liste déroulante, sélectionnez le profil à associer à la valeur que vous avez saisie pour Argument de requête.

Réacheminer une requête vers l'origine lorsque le profil spécifié dans un argument de requête n'existe pas

Sélectionnez la case à cocher pour permettre à la demande d'être acheminée vers votre origine si le profil spécifié dans un argument de requête n'est pas défini dans CloudFront.

Étape 5 : ajouter une configuration à un comportement de cache

Pour utiliser le chiffrement au niveau du champ, associez une configuration à un comportement de cache pour une distribution en ajoutant l'ID de configuration en tant que valeur pour votre distribution.

Important

Pour associer une configuration de chiffrement au niveau du champ à un comportement de cache, la distribution doit être configurée pour toujours utiliser HTTPS et accepter des demandes HTTP `POST` et `PUT` des utilisateurs. Ainsi, les conditions suivantes doivent être vraies :

- La Viewer Protocol Policy (Politique de protocole d'utilisateur) du comportement de cache doit être définie sur Redirect HTTP vers HTTPS (Rediriger HTTP vers HTTPS) ou HTTPS Only (HTTPS uniquement). (Dans CloudFormation ou dans l' CloudFront API, `ViewerProtocolPolicy` elle doit être réglée sur `redirect-to-https` ou`https-only`.)

- Les Allowed HTTP Methods (Méthodes HTTP autorisées) du comportement du cache doivent être définies sur GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE. (Dans CloudFormation ou l' CloudFront API, `AllowedMethods` doit être réglé sur `GETHEAD,OPTIONS,PUT,POST,PATCH,DELETE`. Elles peuvent être spécifiées dans n'importe quel ordre.)
- La Stratégie de protocole d'origine du paramètre d'origine doit être définie sur Identique à l'utilisateur ou HTTPS uniquement. (Dans CloudFormation ou dans l' CloudFront API, `OriginProtocolPolicy` elle doit être réglée sur `match-viewer` ou`https-only`.)

Pour plus d'informations, consultez Référence de tous les paramètres de distribution.

Déchiffrage de champs de données à votre origine

CloudFront chiffre les champs de données à l'aide du AWS Encryption SDK. Les données restent chiffrées dans l'ensemble de votre pile d'applications et ne sont accessibles qu'aux applications possédant les informations d'identification pour les déchiffrer.

Après le chiffrement, le texte chiffré est encodé en base64. Lorsque vos applications déchiffrent le texte à l'origine, elles doivent d'abord décoder le texte chiffré, puis utiliser le kit SDK de chiffrement AWS pour déchiffrer les données.

L'exemple de code suivant illustre la façon dont les applications peuvent déchiffrer des données à votre origine. Remarques :

- Pour simplifier l'exemple, cet exemple charge des clés publiques et privées (au format DER) à partir de fichiers du répertoire de travail. En pratique, vous devez stocker la clé privée à un emplacement sécurisé hors ligne, par exemple un module de sécurité matérielle hors ligne, et distribuer la clé publique à votre équipe de développement.
- CloudFront utilise des informations spécifiques lors du chiffrement des données, et le même ensemble de paramètres doit être utilisé à l'origine pour les déchiffrer. Les paramètres CloudFront utilisés lors de l'initialisation MasterKey sont notamment les suivants :
  - PROVIDER_NAME : Vous avez indiqué cette valeur lors de la création d'un profil de chiffrement au niveau du profil. Utilisez la même valeur ici.
  - KEY_NAME : vous avez créé un nom pour votre clé publique lorsque vous l'avez téléchargée vers CloudFront, puis vous l'avez spécifié dans le profil. Utilisez la même valeur ici.

- ALGORITHME : CloudFront utilisé `RSA/ECB/OAEPWithSHA-256AndMGF1Padding` comme algorithme de chiffrement, vous devez donc utiliser le même algorithme pour déchiffrer les données.

- Si vous exécutez l'exemple de programme suivant avec le texte chiffré en tant qu'entrée, les données déchiffrées constituent une sortie de votre console. Pour plus d'informations, consultez l'exemple de code Java dans le SDK de AWS chiffrement.

Exemple de code

```
import java.nio.file.Files;
import java.nio.file.Paths;
import java.security.KeyFactory;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.spec.PKCS8EncodedKeySpec;
import java.security.spec.X509EncodedKeySpec;

import org.apache.commons.codec.binary.Base64;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CryptoResult;
import com.amazonaws.encryptionsdk.jce.JceMasterKey;

/**
 * Sample example of decrypting data that has been encrypted by CloudFront field-level
 encryption.
 */
public class DecryptExample {

    private static final String PRIVATE_KEY_FILENAME = "private_key.der";
    private static final String PUBLIC_KEY_FILENAME = "public_key.der";
    private static PublicKey publicKey;
    private static PrivateKey privateKey;

    // CloudFront uses the following values to encrypt data, and your origin must use
 same values to decrypt it.
    // In your own code, for PROVIDER_NAME, use the provider name that you specified
 when you created your field-level
    // encryption profile. This sample uses 'DEMO' for the value.
    private static final String PROVIDER_NAME = "DEMO";
```

```
   // In your own code, use the key name that you specified when you added your public
key to CloudFront. This sample
   // uses 'DEMOKEY' for the key name.
   private static final String KEY_NAME = "DEMOKEY";
   // CloudFront uses this algorithm when encrypting data.
   private static final String ALGORITHM = "RSA/ECB/OAEPWithSHA-256AndMGF1Padding";

   public static void main(final String[] args) throws Exception {

       final String dataToDecrypt = args[0];

       // This sample uses files to get public and private keys.
       // In practice, you should distribute the public key and save the private key
in secure storage.
       populateKeyPair();

       System.out.println(decrypt(debase64(dataToDecrypt)));
   }

   private static String decrypt(final byte[] bytesToDecrypt) throws Exception {
       // You can decrypt the stream only by using the private key.

       // 1. Instantiate the SDK
       final AwsCrypto crypto = new AwsCrypto();

       // 2. Instantiate a JCE master key
       final JceMasterKey masterKey = JceMasterKey.getInstance(
               publicKey,
               privateKey,
               PROVIDER_NAME,
               KEY_NAME,
               ALGORITHM);

       // 3. Decrypt the data
       final CryptoResult <byte[], ? > result = crypto.decryptData(masterKey,
bytesToDecrypt);
       return new String(result.getResult());
   }

   // Function to decode base64 cipher text.
   private static byte[] debase64(final String value) {
       return Base64.decodeBase64(value.getBytes());
   }
```

```
    private static void populateKeyPair() throws Exception {
        final byte[] PublicKeyBytes =
 Files.readAllBytes(Paths.get(PUBLIC_KEY_FILENAME));
        final byte[] privateKeyBytes =
 Files.readAllBytes(Paths.get(PRIVATE_KEY_FILENAME));
        publicKey = KeyFactory.getInstance("RSA").generatePublic(new
 X509EncodedKeySpec(PublicKeyBytes));
        privateKey = KeyFactory.getInstance("RSA").generatePrivate(new
 PKCS8EncodedKeySpec(privateKeyBytes));
    }
}
```

Vidéo à la demande et diffusion en direct avec CloudFront

Vous pouvez l'utiliser CloudFront pour diffuser de la vidéo à la demande (VOD) ou du streaming vidéo en direct en utilisant n'importe quelle origine HTTP. Vous pouvez configurer des flux de travail vidéo dans le cloud en les utilisant CloudFront conjointement avec AWS Media Services.

Rubriques

- À propos des vidéos streaming
- Diffusez des vidéos à la demande avec CloudFront
- Diffusez des vidéos en streaming avec CloudFront et AWS Services multimédias
- Résilience tenant compte de la qualité média

À propos des vidéos streaming

Vous devez utiliser un encodeur pour empaqueter le contenu vidéo avant de CloudFront pouvoir distribuer le contenu. Le processus d'empaquetage crée des segments qui contiennent vos contenus audio, vidéo et légendes. Il génère également des fichiers manifestes, qui décrivent dans un ordre spécifique les segments à lire et à quel moment. Les formats courants pour les packages sont MPEG DASH, Apple HLS, Microsoft Smooth Streaming et CMAF.

Streaming VOD

Concernant le streaming VOD, votre contenu vidéo est stocké sur un serveur et les utilisateurs peuvent le regarder à tout moment. Pour créer une ressource que les spectateurs peuvent diffuser, utilisez un encodeur, par exemple AWS Elemental MediaConvert, pour formater et empaqueter vos fichiers multimédias.

Une fois votre vidéo empaquetée dans les bons formats, vous pouvez la stocker sur un serveur ou dans un compartiment Amazon S3, puis la diffuser à CloudFront la demande des spectateurs.

Diffusion de vidéo streaming en direct

Pour la diffusion de vidéo streaming en direct, votre contenu vidéo est diffusé en temps réel au fur et à mesure que les événements en direct se produisent, ou est configuré comme un canal en direct 24/24 , 7/7 j. Pour créer des sorties en direct pour la diffusion et la diffusion en continu, utilisez un encodeur tel que AWS Elemental MediaLive, pour compresser la vidéo et la formater pour les appareils de visualisation.

Une fois votre vidéo encodée, vous pouvez la stocker AWS Elemental MediaStore ou la convertir dans différents formats de diffusion en utilisant AWS Elemental MediaPackage. Utilisez l'une de ces origines pour configurer une CloudFront distribution afin de diffuser le contenu. Pour connaître les étapes spécifiques et les conseils pour créer des distributions fonctionnant avec ces services, consultez Diffusez une vidéo en utilisant AWS Elemental MediaStore comme origine et Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage.

Wowza et Unified Streaming fournissent également des outils que vous pouvez utiliser pour diffuser des vidéos. CloudFront Pour plus d'informations sur l'utilisation de Wowza avec CloudFront, consultez la section Transmettre votre licence Wowza Streaming Engine au streaming HTTP en CloudFront direct sur le site Web de documentation de Wowza. Pour plus d'informations sur l'utilisation du streaming unifié CloudFront pour le streaming VOD, consultez le site Web de documentation CloudFront sur le streaming unifié.

Diffusez des vidéos à la demande avec CloudFront

Pour diffuser de la vidéo à la demande (VOD) en streaming avec CloudFront, utilisez les services suivants :

- Amazon S3 pour stocker le contenu dans son format d'origine et pour stocker la vidéo transcodée.
- Un encodeur (tel que AWS Elemental MediaConvert) pour transcoder la vidéo en formats de streaming.
- CloudFront pour diffuser la vidéo transcodée aux spectateurs. Pour Microsoft Smooth Streaming, consultez Configuration de vidéo à la demande pour Microsoft Smooth Streaming.

Pour créer une solution de VOD avec CloudFront

1. Chargez votre contenu sur un compartiment Amazon S3. Pour en savoir plus sur l'utilisation d'Amazon S3, consultez le Guide de l'utilisateur Amazon Simple Storage Service.
2. Transcodez votre contenu à l'aide d'un MediaConvert job. La tâche convertit votre vidéo dans les formats requis pour les lecteurs que vos spectateurs utilisent. Vous pouvez également utiliser la tâche pour créer des ressources dont la résolution et le débit varient. Ces actifs sont utilisés pour le streaming à débit adaptatif (ABR), qui ajuste la qualité de visionnage en fonction de la bande passante disponible pour le spectateur. MediaConvert stocke la vidéo transcodée dans un compartiment S3.

3. Diffusez votre contenu converti à l'aide d'une CloudFront distribution. Les spectateurs peuvent regarder le contenu sur n’importe quel appareil, à tout moment.

Configuration de vidéo à la demande pour Microsoft Smooth Streaming

Les options suivantes vous permettent de distribuer du contenu vidéo CloudFront à la demande (VOD) que vous avez transcodé au format Microsoft Smooth Streaming :

- Spécifiez un serveur web qui exécute Microsoft IIS et prend en charge Smooth Streaming comme origine de votre distribution.
- Activez Smooth Streaming dans les comportements de cache d'une CloudFront distribution. Étant donné que vous pouvez utiliser plusieurs comportements de cache dans une distribution, vous pouvez utiliser une distribution pour les fichiers multimédias Smooth Streaming ainsi que pour d’autres contenus.

> **Important**
>
> Si vous spécifiez un serveur Web exécutant Microsoft IIS comme origine, n'activez pas Smooth Streaming dans les comportements de cache de votre CloudFront distribution. CloudFront ne pouvez pas utiliser un serveur Microsoft IIS comme origine si vous activez Smooth Streaming en tant que comportement de cache.

Si vous activez Smooth Streaming dans un comportement de cache (c’est-à-dire, si vous n’avez pas de serveur exécutant Microsoft IIS), notez les points suivants :

- Vous pouvez continuer à distribuer d’autres contenus à l’aide du même comportement de cache si le contenu correspond à la valeur de Modèle de chemin pour ce comportement de cache.
- CloudFront peut utiliser un compartiment Amazon S3 ou une origine personnalisée pour les fichiers multimédia Smooth Streaming. CloudFront ne peut pas utiliser un serveur Microsoft IIS comme origine si vous activez Smooth Streaming pour le comportement du cache.
- Vous ne pouvez pas invalider les fichiers multimédias au format Smooth Streaming. Si vous voulez mettre à jour les fichiers avant qu’ils n’expirent, vous devez les renommer. Pour plus d’informations, consultez Ajouter, supprimer ou remplacer le contenu qui CloudFront distribue.

Pour plus d'informations sur les clients Smooth Streaming, consultez Smooth Streaming sur le site web de Microsoft.

À utiliser CloudFront pour distribuer des fichiers Smooth Streaming lorsqu'un serveur Web Microsoft IIS n'est pas l'origine

1. Transcodez vos fichiers multimédias au format MP4 fragmenté Smooth Streaming.
2. Effectuez l'une des actions suivantes :
   - Si vous utilisez la CloudFront console : lorsque vous créez ou mettez à jour une distribution, activez Smooth Streaming dans un ou plusieurs comportements de cache de la distribution.
   - Si vous utilisez l' CloudFront API : ajoutez l'`SmoothStreaming`élément au type `DistributionConfig` complexe pour un ou plusieurs comportements de cache de la distribution.
3. Chargez les fichiers Smooth Streaming vers votre origine.
4. Créez un fichier `clientaccesspolicy.xml` ou `crossdomainpolicy.xml`, puis ajoutez-le à un emplacement accessible à la racine de votre distribution : par exemple, `https://d111111abcdef8.cloudfront.net/clientaccesspolicy.xml`. Voici un exemple de politique :

   ```
   <?xml version="1.0" encoding="utf-8"?>
   <access-policy>
   <cross-domain-access>
   <policy>
   <allow-from http-request-headers="*">
   <domain uri="*"/>
   </allow-from>
   <grant-to>
   <resource path="/" include-subpaths="true"/>
   </grant-to>
   </policy>
   </cross-domain-access>
   </access-policy>
   ```

   Pour plus d'informations, consultez Making a Service Available Across Domain Boundaries sur le site web Microsoft Developer Network.
5. Pour les liens dans votre application (un lecteur multimédia, par exemple), spécifiez l'URL du fichier multimédia au format suivant :

```
https://d111111abcdef8.cloudfront.net/video/presentation.ism/Manifest
```

Diffusez des vidéos en streaming avec CloudFront et AWS Services multimédias

Pour utiliser AWS Media Services avec CloudFront afin de diffuser du contenu en direct à un public mondial, consultez les instructions suivantes.

Utilisez AWS Elemental MediaLive pour encoder les flux vidéo en direct en temps réel. Pour encoder un flux vidéo volumineux, MediaLive compressez-le en versions plus petites (encodages) qui peuvent être distribuées à vos spectateurs.

Après avoir compressé un flux vidéo en direct, vous disposez des deux options principales suivantes pour préparer et diffuser le contenu :

- Convertissez votre contenu dans les formats requis, puis diffusez-le : si vous avez besoin de contenu dans plusieurs formats, utilisez AWS Elemental MediaPackage pour empaqueter le contenu pour différents types d'appareils. Lorsque vous empaquetez le contenu, vous pouvez également implémenter des fonctionnalités supplémentaires et ajouter la gestion des droits numériques (DRM) pour empêcher l'utilisation non autorisée de votre contenu. Pour obtenir des instructions détaillées sur l'utilisation CloudFront pour diffuser du contenu MediaPackage mis en forme, consultezDiffusez des vidéos en direct formatées avec AWS Elemental MediaPackage.
- Stockez et diffusez votre contenu en utilisant une origine évolutive — Si le contenu est MediaLive codé dans les formats requis par tous les appareils utilisés par vos spectateurs, utilisez une origine hautement évolutive, comme AWS Elemental MediaStore pour diffuser le contenu. Pour obtenir des instructions détaillées CloudFront sur l'utilisation pour diffuser du contenu stocké dans un MediaStore conteneur, consultezDiffusez une vidéo en utilisant AWS Elemental MediaStore comme origine.

Une fois que vous avez configuré votre origine à l'aide de l'une de ces options, vous pouvez distribuer la vidéo en streaming en direct aux utilisateurs en utilisant CloudFront.

> **Tip**
>
> Vous pouvez en savoir plus sur une AWS solution qui déploie automatiquement des services pour créer une expérience de visionnage en temps réel hautement disponible. Pour connaître

les étapes permettant de déployer automatiquement cette solution, consultez Déploiement automatisé de streaming en direct.

Rubriques

- Diffusez une vidéo en utilisant AWS Elemental MediaStore comme origine
- Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage
- Diffusez du contenu vidéo à la demande avec AWS Elemental MediaPackage

Diffusez une vidéo en utilisant AWS Elemental MediaStore comme origine

Si vous avez une vidéo stockée dans un AWS Elemental MediaStore conteneur, vous pouvez créer une CloudFront distribution pour diffuser le contenu.

Pour commencer, vous autorisez CloudFront l'accès à votre MediaStore conteneur. Vous créez ensuite une CloudFront distribution et vous la configurez pour qu'elle fonctionne avec MediaStore.

Pour diffuser du contenu à partir d'un AWS Elemental MediaStore conteneur

1. Suivez la procédure décrite dans Autoriser Amazon CloudFront à accéder à votre AWS Elemental MediaStore conteneur, puis revenez à ces étapes pour créer votre distribution.
2. Créez une distribution avec les paramètres suivants :

   a. Domaine d'origine : point de terminaison de données attribué à votre MediaStore conteneur. Dans la liste déroulante, choisissez le MediaStore conteneur pour votre vidéo en direct.

   b. Chemin d'origine : structure de dossiers du MediaStore conteneur dans lequel sont stockés vos objets. Pour plus d'informations, consultez the section called “Chemin d'origine”.

   c. Ajouter un en-tête personnalisé : ajoutez des noms et des valeurs d'en-tête si vous CloudFront souhaitez ajouter des en-têtes personnalisés lorsque les demandes sont transmises à votre origine.

   d. Politique de protocole d'utilisateur : choisissez Rediriger HTTP vers HTTPS. Pour plus d'informations, consultez the section called “Viewer Protocol Policy”.

   e. Politique de cache et Politique de demande d'origine

      - PourCache policy (Politique de cache), choisissez Create policy (Créer une politique), puis créez une politique de cache adaptée à vos besoins de mise en cache et aux durées

de segment. Une fois la politique créée, actualisez la liste des politiques de cache et choisissez la politique que vous venez de créer.

- Pour la politique relative aux requêtes Origin, choisissez CORS-CustomOrigin dans la liste déroulante.

Pour les autres paramètres, vous pouvez définir des valeurs spécifiques selon d'autres exigences techniques ou selon les besoins de votre entreprise. Afin d'obtenir une liste de toutes les options pour les distributions ainsi que leurs informations de configuration, veuillez consulter the section called "Tous les paramètres de distribution".

3. Pour les liens de votre application (par exemple, un lecteur multimédia), spécifiez le nom du fichier multimédia dans le même format que celui que vous utilisez pour les autres objets que vous distribuez CloudFront.

Diffusez des vidéos en direct formatées avec AWS Elemental MediaPackage

Si vous avez formaté une diffusion en direct à l'aide de AWS Elemental MediaPackage, vous pouvez créer une CloudFront distribution et configurer les comportements du cache pour diffuser la diffusion en direct. Le processus suivant implique que vous avez déjà créé un canal et ajouté des points de terminaison pour vos vidéos en direct en utilisant MediaPackage.

Pour créer une CloudFront distribution pour MediaPackage manuellement, procédez comme suit :

Étape 1 : Création et configuration d'une CloudFront distribution

Suivez la procédure suivante pour configurer une CloudFront distribution pour la chaîne vidéo en direct que vous avez créée avec MediaPackage.

Pour créer une distribution pour votre canal vidéo en direct

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Créer une distribution.
3. Choisissez les paramètres de la distribution, en particulier les suivants :

Domaine de l’origine

L'origine de votre chaîne vidéo MediaPackage en direct et de vos points de terminaison. Choisissez le champ de texte, puis, dans la liste déroulante, choisissez le domaine MediaPackage d'origine de votre vidéo en direct. Vous pouvez mapper un domaine à plusieurs points de terminaison d'origine.

Si vous avez créé votre domaine d'origine à partir d'un autre compte AWS , saisissez la valeur d'URL de l'origine dans le champ. L’origine doit être une URL HTTPS.

Par exemple, pour un point de terminaison HLS comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, le domaine d'origine est `3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com`.

Pour plus d’informations, consultez the section called “Domaine d'origine”.

Chemin d’origine

Le chemin vers le MediaPackage point de terminaison à partir duquel le contenu est diffusé.

Pour plus d’informations sur le fonctionnement d’un chemin d’origine, consultez the section called “Chemin d’origine”.

> **Important**
>
> Le chemin générique `*` est obligatoire pour acheminer quelque part dans la CloudFront distribution. Pour éviter que les requêtes qui ne correspondent pas à un chemin explicite ne soient routées vers l'origine réelle, créez une origine « fictive » pour ce chemin générique.

Example: Création d'une origine « fictive »

Si, dans l'exemple suivant, les points de terminaison `abc123` et `def456` routent vers l'origine « réelle », les demandes de contenu vidéo de tout autre point de terminaison sont routées vers `mediapackage.us-west-2.amazonaws.com` sans le sous-domaine approprié, ce qui entraîne un HTTP `404`.

MediaPackage points de terminaison :

```
https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/
index.m3u8
https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/def456/
index.m3u8
```

CloudFront Origine A :

```
Domain: 3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com
Path: None
```

CloudFront Origine B :

```
Domain: mediapackage.us-west-2.amazonaws.com
Path: None
```

CloudFront comportement du cache :

```
1. Path: /out/v1/abc123/* forward to Origin A
2. Path: /out/v1/def456/* forward to Origin A
3. Path: * forward to Origin B
```

Pour les autres paramètres de distribution, définissez des valeurs spécifiques en fonction des autres exigences techniques ou des besoins de votre entreprise. Afin d'obtenir une liste de toutes les options pour les distributions ainsi que leurs informations de configuration, consultez the section called "Tous les paramètres de distribution".

Lorsque vous avez terminé de choisir les autres paramètres de distribution, choisissez Create distribution (Créer une distribution).

4. Choisissez la distribution que vous venez de créer, puis choisissez Behaviors (Comportements).
5. Sélectionnez le comportement du cache par défaut, puis choisissez Edit (Modifier). Spécifiez les paramètres de comportement du cache corrects pour le canal que vous avez choisi pour l'origine. Vous ajouterez ensuite une ou plusieurs autres origines supplémentaires et modifierez les paramètres de comportement du cache pour ces origines.
6. Accédez à la page CloudFront des distributions.

7. Attendez que la valeur de la colonne Dernière modification pour votre distribution passe de Déploiement à une date et une heure, indiquant que votre distribution CloudFront a été créée.

Étape 2 : Ajoutez Origins aux domaines de vos MediaPackage terminaux

Répétez les étapes ci-dessous pour ajouter chacun des points de terminaison de votre MediaPackage chaîne à votre distribution, en gardant à l'esprit la nécessité de créer une origine « fictive ».

Pour ajouter d’autres points de terminaison en tant qu’origines

1. Sur la CloudFront console, choisissez la distribution que vous avez créée pour votre chaîne.
2. Choisissez Origins (Origines), puis Create origin (Créer une origine).
3. Pour le domaine Origin, dans la liste déroulante, choisissez un MediaPackage point de terminaison pour votre chaîne.
4. Pour les autres paramètres, définissez les valeurs en fonction des autres exigences techniques ou des besoins de votre entreprise. Pour plus d’informations, consultez the section called “Paramètres d’origine”.
5. Choisissez Create origin (Créer une origine).

Étape 3 : configurer les comportements de cache pour tous les points de terminaison

Pour chaque point de terminaison, vous devez configurer les comportements de cache pour ajouter des modèles de chemin qui acheminent les requêtes correctement. Les modèles de chemin que vous spécifiez dépendent du format vidéo que vous diffusez. La procédure suivante inclut les informations de modèle de chemin à utiliser pour les formats Apple HLS, CMAF, DASH et Microsoft Smooth Streaming.

Vous configurez généralement deux comportements de cache pour chaque point de terminaison :

- Le manifeste parent, qui est l’index pour vos fichiers.
- Les segments, qui sont les fichiers du contenu vidéo.

Pour créer un comportement de cache pour un point de terminaison

1. Sur la CloudFront console, choisissez la distribution que vous avez créée pour votre chaîne.
2. Choisissez Behaviors (Comportements), puis Create Behavior (Créer un comportement).

3. Pour le modèle de chemin, utilisez un MediaPackage `OriginEndpoint` GUID spécifique comme préfixe de chemin.

   Modèles de chemin

   Pour un point de terminaison HLS
   comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, créez les deux comportements de cache suivants :

   - Pour les manifestes parents et enfants, utilisez `/out/v1/abc123/*.m3u8`.
   - Pour les segments de contenu, utilisez `/out/v1/abc123/*.ts`.

   Pour un point de terminaison CMAF
   comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.m3u8`, créez les deux comportements de cache suivants :

   - Pour les manifestes parents et enfants, utilisez `/out/v1/abc123/*.m3u8`.
   - Pour les segments de contenu, utilisez `/out/v1/abc123/*.mp4`.

   Pour un point de terminaison DASH
   comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.mpd`, créez les deux comportements de cache suivants :

   - Pour le manifeste parent, utilisez `/out/v1/abc123/*.mpd`.
   - Pour les segments de contenu, utilisez `/out/v1/abc123/*.mp4`.

   Pour un point de terminaison Microsoft Smooth Streaming
   comme `https://3ae97e9482b0d011.mediapackage.us-west-2.amazonaws.com/out/v1/abc123/index.ism`, seul un manifeste est diffusé. Vous ne créez donc qu'un seul comportement de cache : `out/v1/abc123/index.ism/*`.

4. Renseignez les valeurs des paramètres suivants pour chaque comportement de cache :

   Viewer Protocol Policy

   Choisissez Rediriger HTTP vers HTTPS.

   Politique de cache et politique de demande d'origine

   Pour Cache policy (Politique de cache), choisissez Create policy (Créer une poliltique). Pour votre nouvelle politique de cache, spécifiez les paramètres suivants :

Durée de vie minimale

Définissez sur 5 secondes ou moins pour éviter la diffusion de contenu obsolète.

Chaînes de requête

Pour Query strings (Chaînes de requête) (dans Cache key settings (Paramètres de clé de cache), choisissez Include specified query strings (Inclure des chaînes de requête spécifiées). Pour Allow (Autoriser), ajoutez les valeurs suivantes en les saisissant, puis choisissez Add item (Ajouter un élément) :

- Ajoutez `m` en tant que chaîne de requête le paramètre que vous CloudFront souhaitez utiliser comme base pour la mise en cache. La MediaPackage réponse inclut toujours la balise permettant `?m=###` de capturer l'heure modifiée du point de terminaison. Si le contenu est déjà mis en cache avec une valeur différente pour cette balise, CloudFront demande un nouveau manifeste au lieu de diffuser la version mise en cache.
- Si vous utilisez la fonctionnalité d'affichage décalé dans le temps de MediaPackage, spécifiez `start` et en `end` tant que paramètres de chaîne de requête supplémentaires sur le comportement du cache pour les demandes de manifeste (`*.m3u8`*`.mpd`, et`index.ism/*`). De cette façon, le contenu diffusé est spécifique à la période demandée dans la requête de manifeste. Pour plus d'informations sur l'affichage décalé dans le temps et le formatage des paramètres de demande de début et de fin du contenu, consultez la section Time-shifted Affichage dans le Guide de AWS Elemental MediaPackage l'utilisateur.
- Si vous utilisez la fonctionnalité de filtrage des manifestes dans MediaPackage, spécifiez `aws.manifestfilter` comme paramètre de chaîne de requête supplémentaire la politique de cache que vous utilisez avec le comportement du cache pour les demandes de manifeste (`*.m3u8`*`.mpd`, et`index.ism/*`). Cela configure votre distribution pour qu'elle transmette la chaîne de `aws.manifestfilter` requête à votre MediaPackage origine, ce qui est requis pour que la fonctionnalité de filtrage des manifestes fonctionne. Pour en savoir plus, consultez Filtrage des manifestes dans le Guide de l'utilisateur AWS Elemental MediaPackage .
- Si vous utilisez HLS (LL-HLS) à faible latence, spécifiez `_HLS_msn` et en `_HLS_part` tant que paramètres de chaîne de requête supplémentaires pour la politique de cache que vous utilisez avec le comportement du cache pour les requêtes de manifeste ()`*.m3u8`. Cela configure votre distribution pour transférer les chaînes `_HLS_msn` et les `_HLS_part` requêtes vers votre MediaPackage origine, ce qui est nécessaire pour que la fonctionnalité de LL-HLS blocage des demandes de playlist fonctionne.

5. Cliquez sur Créer.
6. Après avoir créé la politique de cache, revenez au flux de création de comportements de cache. Actualisez la liste des politiques de cache, puis choisissez la politique que vous venez de créer.
7. Choisissez Create behavior (Créer un comportement).
8. Si votre point de terminaison n'est pas un point de terminaison Microsoft Smooth Streaming, répétez ces étapes pour créer un second comportement de cache.

Étape 4 : Activer l'autorisation CDN basée sur les en-têtes MediaPackage

Nous vous recommandons d'activer l'autorisation MediaPackage CDN basée sur les en-têtes entre les MediaPackage terminaux et la distribution. CloudFront Pour plus d'informations, consultez la section Activer l'autorisation CDN MediaPackage dans le Guide de l'AWS Elemental MediaPackage utilisateur.

Étape 5 : Utiliser CloudFront pour diffuser la chaîne de diffusion en direct

Après avoir créé la distribution, ajouté les origines, créé les comportements de cache et activé l'autorisation CDN basée sur les en-têtes, vous pouvez diffuser le canal de diffusion en direct en utilisant. CloudFront CloudFront achemine les demandes des spectateurs vers les MediaPackage points de terminaison appropriés en fonction des paramètres que vous avez configurés pour les comportements du cache.

Pour les liens de votre application (par exemple, un lecteur multimédia), spécifiez l'URL du fichier multimédia au format standard pour CloudFront les URL. Pour plus d'informations, consultez the section called "Personnalisation des URL de fichier".

Diffusez du contenu vidéo à la demande avec AWS Elemental MediaPackage

Si votre contenu de vidéo à la demande (VOD) provient AWS Elemental MediaPackage d'une origine, vous pouvez créer une CloudFront distribution et configurer des comportements de cache optimisés pour diffuser le contenu VOD aux spectateurs. Le processus suivant part du principe que vous avez déjà créé un groupe d'empaquetage avec une configuration d'empaquetage et que vous avez ingéré un actif avec MediaPackage.

Pour créer une CloudFront distribution pour MediaPackage manuellement, procédez comme suit :

Étape 1 : Création et configuration d'une CloudFront distribution

Suivez la procédure suivante pour configurer une CloudFront distribution pour le groupe d'emballages que vous avez créé avec MediaPackage.

Pour créer une distribution pour votre contenu VOD

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Créer une distribution.
3. Choisissez les paramètres de la distribution, en particulier les suivants :

   Domaine de l'origine

   L'origine de votre groupe MediaPackage d'emballages. Entrez la valeur de l'URL d'origine dans le champ de texte. L'origine doit être une URL HTTPS.

   Par exemple, pour un point de terminaison HLS comme `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, le domaine d'origine est `3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com`.

   Pour plus d'informations, consultez the section called "Domaine d'origine".

   Chemin d'origine

   Chemin d'accès à partir duquel le contenu est diffusé.

   Pour plus d'informations sur le fonctionnement d'un chemin d'origine, consultez the section called "Chemin d'origine".

> **Important**
>
> Le chemin générique * est obligatoire pour acheminer quelque part dans la CloudFront distribution. Pour éviter que les requêtes qui ne correspondent pas à un chemin explicite ne soient routées vers l'origine réelle, créez une origine « fictive » pour ce chemin générique.

Example: Création d'une origine « fictive »

Dans l'exemple suivant, les configurations d'empaquetage `def456` et `321xyz` sont dirigées vers l'origine « réelle », mais les demandes pour tout autre contenu vidéo sont acheminées vers `mediapackage-vod.us-west-2.amazonaws.com` sans le sous-domaine approprié, ce qui entraîne une erreur HTTP `404`.

MediaPackage URL de contenu pour une ressource unique pour un groupe de packages avec deux configurations d'emballage :

```
https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/
abc123/def456/ghi789/index.m3u8
https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/
abc123/321xyz/654uvw/index.m3u8
```

CloudFront Origine A :

```
Domain: 3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com
Path: None
```

CloudFront Origine B :

```
Domain: mediapackage-vod.us-west-2.amazonaws.com
Path: None
```

CloudFront comportement du cache :

```
1. Path: /out/v1/*/def456/* forward to Origin A
2. Path: /out/v1/*/321xyz/* forward to Origin A
3. Path: * forward to Origin B
```

Pour les autres paramètres de distribution, définissez des valeurs spécifiques en fonction des autres exigences techniques ou des besoins de votre entreprise. Afin d'obtenir une liste de toutes les options pour les distributions ainsi que leurs informations de configuration, consultez the section called "Tous les paramètres de distribution".

Lorsque vous avez terminé de choisir les autres paramètres de distribution, choisissez Create distribution (Créer une distribution).

4. Choisissez la distribution que vous venez de créer, puis choisissez Behaviors (Comportements).
5. Sélectionnez le comportement du cache par défaut, puis choisissez Edit (Modifier). Spécifiez les paramètres de comportement du cache corrects pour la configuration d'empaquetage que vous avez choisie pour l'origine. Vous ajouterez ensuite une ou plusieurs autres origines supplémentaires et modifierez les paramètres de comportement du cache pour ces origines.
6. Accédez à la page CloudFront des distributions.
7. Attendez que la valeur de la colonne Dernière modification pour votre distribution passe de Déploiement à une date et une heure, indiquant que votre distribution CloudFront a été créée.

Étape 2 : Ajoutez Origins pour les domaines de vos groupes MediaPackage d'emballages

Répétez les étapes ci-dessous pour ajouter chacun de vos groupes MediaPackage d'emballages à votre distribution, en gardant à l'esprit la nécessité de créer une origine « fictive ».

Pour ajouter d'autres groupes d'empaquetage en tant qu'origines

1. Sur la CloudFront console, choisissez la distribution que vous avez créée pour votre chaîne.
2. Choisissez Origins (Origines), puis Create origin (Créer une origine).
3. Pour le domaine d'origine, saisissez l'URL du groupe de MediaPackage packaging.
4. Pour les autres paramètres, définissez les valeurs en fonction des autres exigences techniques ou des besoins de votre entreprise. Pour plus d'informations, consultez the section called "Paramètres d'origine".
5. Choisissez Create origin (Créer une origine).

Étape 3 : configurer les comportements de cache pour toutes les configurations d'empaquetage

Pour chaque configuration d'empaquetage, vous devez configurer les comportements de cache pour ajouter des modèles de chemin qui acheminent les demandes correctement. Les modèles de chemin que vous spécifiez dépendent du format vidéo que vous diffusez. La procédure suivante inclut les informations de modèle de chemin à utiliser pour les formats Apple HLS, CMAF, DASH et Microsoft Smooth Streaming.

Vous configurez généralement plusieurs comportements de cache pour chaque configuration d'empaquetage :

- Le manifeste parent, qui est l'index pour vos fichiers.
- Les segments, qui sont les fichiers du contenu vidéo. Un format peut utiliser plusieurs extensions pour le contenu, en fonction de votre configuration. Un comportement de cache est nécessaire pour chaque extension.

Pour créer un comportement de cache pour une configuration d'empaquetage

1. Sur la CloudFront console, choisissez la distribution que vous avez créée pour votre chaîne.
2. Choisissez Behaviors (Comportements), puis Create Behavior (Créer un comportement).
3. Pour le modèle de chemin, utilisez un GUID de configuration d'emballage MediaPackage VOD spécifique comme préfixe de chemin. Il s'agit du deuxième GUID d'un chemin MediaPackage VOD.

   Modèles de chemin

   Pour du contenu HLS comme `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, créez les comportements de cache suivants :

   - Pour les manifestes parents et enfants, utilisez `/out/v1/*/def456/*.m3u8`.
   - Pour les segments de contenu, utilisez `/out/v1/*/def456/*.ts` et répétez pour toutes les extensions de segment nécessaires.

   Pour du contenu CMAF comme `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.m3u8`, créez les comportements de cache suivants :

   - Pour les manifestes parents et enfants, utilisez `/out/v1/*/def456/*.m3u8`.
   - Pour les segments de contenu, utilisez `/out/v1/*/def456/*.mp4` et répétez pour toutes les extensions de segment nécessaires.

   Pour du contenu DASH comme `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.mpd`, créez les comportements de cache suivants :

   - Pour le manifeste parent, utilisez `/out/v1/*/def456/*.mpd`.
   - Pour les segments de contenu, utilisez `/out/v1/*/def456/*.mp4`.

Pour un point de terminaison Microsoft Smooth Streaming comme `https://3ae97e9482b0d011.egress.mediapackage-vod.us-west-2.amazonaws.com/out/v1/abc123/def456/ghi789/index.ism/Manifest`, seul un manifeste est diffusé. Vous ne créez donc qu'un seul comportement de cache : `out/v1/*/def456/*/index.ism/*`.

4. Renseignez les valeurs des paramètres suivants pour chaque comportement de cache :

   Viewer Protocol Policy

   Choisissez Rediriger HTTP vers HTTPS.

   Politique de cache et politique de demande d'origine

   Pour Cache policy (Politique de cache), choisissez Create policy (Créer une poliltique). Pour votre nouvelle politique de cache, spécifiez les paramètres suivants :

   Durée de vie minimale

   Définissez sur 5 secondes ou moins pour éviter la diffusion de contenu obsolète.

   Chaînes de requête

   Pour Query strings (Chaînes de requête) (dans Cache key settings (Paramètres de clé de cache), choisissez Include specified query strings (Inclure des chaînes de requête spécifiées). Pour Allow (Autoriser), ajoutez les valeurs suivantes en les saisissant, puis choisissez Add item (Ajouter un élément) :

   - Si vous utilisez la fonctionnalité de filtrage des manifestes dans MediaPackage, spécifiez `aws.manifestfilter` comme paramètre de chaîne de requête supplémentaire la politique de cache que vous utilisez avec le comportement du cache pour les demandes de manifeste (`*.m3u8*.mpd`, et`index.ism/*`). Cela configure votre distribution pour transmettre la chaîne de `aws.manifestfilter` requête à votre MediaPackage origine, ce qui est requis pour que la fonctionnalité de filtrage des manifestes fonctionne. Pour en savoir plus, consultez Filtrage des manifestes dans le Guide de l'utilisateur AWS Elemental MediaPackage .

5. Cliquez sur Créer.
6. Après avoir créé la politique de cache, revenez au flux de création de comportements de cache. Actualisez la liste des politiques de cache, puis choisissez la politique que vous venez de créer.
7. Choisissez Create behavior (Créer un comportement).

8. Si votre point de terminaison n’est pas un point de terminaison Microsoft Smooth Streaming, répétez ces étapes pour créer un second comportement de cache.

Étape 4 : Activer l'autorisation CDN basée sur les en-têtes MediaPackage

Nous vous recommandons d'activer l'autorisation MediaPackage CDN basée sur les en-têtes entre le contenu MediaPackage VOD et la distribution. CloudFront Pour plus d'informations, consultez la section Activer l'autorisation CDN MediaPackage dans le Guide de l'AWS Elemental MediaPackage utilisateur.

Étape 5 : Utiliser CloudFront pour diffuser le contenu VOD

Après avoir créé la distribution, ajouté les origines, créé les comportements de cache et activé l'autorisation CDN basée sur les en-têtes, vous pouvez diffuser le contenu VOD en utilisant. CloudFront CloudFront achemine les demandes des spectateurs vers le contenu MediaPackage VOD approprié en fonction des paramètres que vous avez configurés pour les comportements du cache.

Pour les liens de votre application (par exemple, un lecteur multimédia), spécifiez l'URL du fichier multimédia au format standard pour CloudFront les URL. Pour plus d’informations, consultez the section called “Personnalisation des URL de fichier”.

Résilience tenant compte de la qualité média

La résilience axée sur la qualité des médias (MQAR) est une fonctionnalité intégrée entre Amazon CloudFront et Media Services. AWS La MQAR fournit une sélection automatisée d’origine inter-régions basée sur le score de confiance de la qualité média (MQCS). Le MQCS est synthétisé par AWS Elemental MediaLive en fonction des paramètres qui influencent l’expérience de qualité média perçue par les utilisateurs. Vous pouvez configurer CloudFront et AWS Media Services pour diffuser vos événements en direct avec une résilience élevée en utilisant plusieurs options que vous pouvez spécifier dans les critères de basculement du groupe CloudFront d'origine.

Lorsque vous activez la fonctionnalité MQAR pour votre distribution, vous autorisez CloudFront à sélectionner automatiquement l'origine considérée comme ayant le score de qualité le plus élevé.

Le score de qualité représente les problèmes de qualité perçus dans la diffusion de vos contenus médias depuis vos origines, tels que des écrans noirs, des images figées ou perdues, ou encore des images répétées. Par exemple, si vos origines AWS Elemental MediaPackage v2 sont déployées dans deux versions différentes Régions AWS et que l'une affiche un score de qualité multimédia plus

élevé que l'autre, CloudFront vous passerez automatiquement à l'origine qui affiche le score le plus élevé.

Pour ce faire, CloudFront procédez comme suit :

1. CloudFront transmet une `GET` demande à l' MediaPackage origine principale et lance également une `HEAD` demande à l' MediaPackage origine secondaire en même temps. CloudFront reçoit le score de qualité multimédia dans les en-têtes de réponse de chaque origine.
2. Ensuite, CloudFront suit le score pour chaque origine et utilise ces informations pour déterminer l'origine ayant le score le plus élevé lorsqu'une nouvelle demande arrive.

Le score de qualité multimédia de vos origines peut changer en temps réel. CloudFront détermine cela en consommant les modifications du MQCS et passe d'une origine à l'autre pour s'assurer que les spectateurs voient le contenu multimédia de meilleure qualité. Pour plus d'informations, consultez la section Tirer parti des scores de qualité multimédia MediaPackage dans le Guide de l'utilisateur de la AWS Elemental MediaPackage V2.

Le MQAR aide à CloudFront déterminer, le plus tôt possible, s'il existe un problème susceptible d'avoir un impact sur les clients. Par exemple, des problèmes tels que la connexion réseau, le traitement vidéo, la perte ou la coupure audio, ou encore des problèmes de vitesse de l'encodeur peuvent affecter le score de qualité média pour vos utilisateurs.

MQAR permet une commutation fluide entre les origines, ce qui vous permet de déployer un flux de diffusion multimédia de bout en bout résilient et interrégional sur AWS et de fournir un contenu de qualité à vos spectateurs.

> **Note**
>
> Actuellement, cette fonctionnalité ne prend en charge que les origines MediaPackage v2.

Pour activer cette fonctionnalité pour votre distribution, procédez comme suit :

1. Si ce n'est pas déjà fait, créez vos origines MediaPackage v2 et activez cette fonctionnalité dans la configuration de votre terminal. Pour un déploiement interrégional, créez un canal secondaire dans un autre canal Région AWS avec les mêmes paramètres. Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur AWS Elemental MediaPackage V2 :
   - Création d'un canal et d'un point de terminaison

- Activation du score de qualité média

2. Pour utiliser vos origines MediaPackage v2 CloudFront, créez ou mettez à jour une CloudFront distribution. Consultez Créer une distribution et Mettre à jour une distribution.
3. Créez un groupe d'origines, puis désignez vos deux origines comme primaire et secondaire. Dans votre groupe d'origines, activez l'option Score de qualité multimédia. Pour plus d'informations, consultez Création d'un groupe d'origine.
4. Dans le comportement de cache de votre distribution, sélectionnez le groupe d'origines que vous avez créé. Nous recommandons que le comportement de cache corresponde au modèle de chemin du canal.

Si elle CloudFront détermine que les deux origines MediaPackage v2 ont le même score, elle transmet la demande à l'origine principale répertoriée dans le groupe d'origine. Si l'origine initialement sélectionnée répond par un code d'erreur correspondant aux critères de basculement que vous avez spécifiés dans votre groupe d'origine, essayez à CloudFront nouveau la demande vers l'origine alternative de votre groupe d'origine, quel que soit son score de qualité multimédia.

Remarques

- CloudFront suit le score de qualité pour chaque comportement de cache qui utilise un groupe d'origine activé pour le score de qualité multimédia. Si le même groupe d'origines est utilisé pour plusieurs canaux qui émettent un score de qualité média, créez un comportement de cache distinct pour le modèle de chemin de chaque canal afin d'éviter de mélanger leurs scores. Pour plus d'informations sur les quotas des groupes d'origines, consultez Quotas généraux sur les distributions.
- Actuellement, la MQAR n'est pas disponible lorsque vous utilisez une fonction Lambda@Edge sur des déclencheurs côté origine (demande à l'origine et réponse de l'origine) associée au comportement de cache de votre distribution. Pour plus d'informations, consultez Paramètres de comportement du cache.
- Si vous avez activé la fonctionnalité MQAR et le contrôle d'accès d'origine (OAC), ajoutez l'action `mediapackagev2:GetHeadObject` à la politique IAM. MQAR a besoin de cette autorisation pour envoyer `HEAD` des requêtes à l'origine MediaPackage v2. Pour plus d'informations sur l'OAC, consultez Restreindre l'accès à une origine AWS Elemental MediaPackage v2.

Champs de journal MQAR

CloudFront fournit les champs suivants dans les journaux d'accès en temps réel pour refléter le score de qualité et l'origine sélectionnée. Vous pouvez activer ces champs dans vos journaux d'accès CloudFront en temps réel :

- `r-host`
- `sr-reason`
- `x-edge-mqcs`

Pour plus d’informations, consultez Champs 65-67.

Personnalisation en périphérie à l’aide de fonctions

Avec Amazon CloudFront, vous pouvez écrire votre propre code pour personnaliser la façon dont vos CloudFront distributions traitent les requêtes et les réponses HTTP. Le code s'exécute à proximité de vos utilisateurs pour minimiser la latence, et vous n'avez pas à gérer de serveurs ou toute autre infrastructure. Vous pouvez écrire du code pour manipuler les demandes et les réponses qui circulent CloudFront, effectuer une authentification et une autorisation de base, générer des réponses HTTP à la périphérie, etc.

Le code que vous écrivez et associez à votre CloudFront distribution s'appelle une fonction Edge. CloudFront propose deux méthodes pour écrire et gérer des fonctions Edge :

CloudFront Fonctions

Vous pouvez y écrire des fonctions légères JavaScript pour des personnalisations CDN à grande échelle et sensibles à la latence. L'environnement d'exécution CloudFront Functions offre des temps de démarrage inférieurs à la milliseconde, s'adapte immédiatement pour gérer des millions de requêtes par seconde et est hautement sécurisé. CloudFront Functions est une fonctionnalité native de CloudFront, ce qui signifie que vous pouvez créer, tester et déployer votre code entièrement depuis CloudFront.

Lambda@Edge

Lambda@Edge est une extension d’AWS Lambda qui offre un calcul puissant et flexible pour des fonctions complexes, ainsi qu’une logique d’application complète plus proche de vos utilisateurs. Le service est hautement sécurisé. Les fonctions Lambda @Edge s'exécutent dans un environnement d'exécution Node.js ou Python. Vous les publiez en une seule fois Région AWS, mais lorsque vous associez la fonction à une CloudFront distribution, Lambda @Edge réplique automatiquement votre code dans le monde entier.

CloudFront Fonctions de connexion

Vous pouvez écrire des JavaScript fonctions légères qui s'exécutent lors de l'établissement de liens de connexion mTLS pour valider les certificats clients, implémenter une logique d'authentification personnalisée et gérer la révocation des certificats. Comme CloudFront les fonctions, les fonctions de connexion sont une fonctionnalité native dans CloudFront laquelle vous pouvez créer, tester et déployer entièrement CloudFront. Pour plus d’informations, consultez Personnalisez avec les fonctions CloudFront de connexion.

Si vous exécutez AWS WAF CloudFront, vous pouvez utiliser des en-têtes AWS WAF insérés à la fois pour CloudFront Functions et Lambda @Edge. Cela fonctionne pour les demandes et réponses des utilisateurs et de l'origine.

Rubriques

- Différences entre CloudFront Functions et Lambda @Edge
- Personnalisez à la périphérie avec CloudFront Functions
- Personnalisez avec les fonctions CloudFront de connexion
- Personnalisation en périphérie avec Lambda@Edge
- Restrictions sur les fonctions périphériques

Différences entre CloudFront Functions et Lambda @Edge

CloudFront Functions et Lambda @Edge permettent tous deux d'exécuter du code en réponse à CloudFront des événements.

CloudFront Functions est idéal pour les fonctions légères et de courte durée dans les cas d'utilisation suivants :

- Normalisation de la clé de cache : transformez les attributs de demandes HTTP (en-têtes, chaînes de requêtes, cookies et même le chemin de l'URL) pour créer une clé de cache optimale, ce qui peut améliorer le taux d'accès à votre cache.
- Manipulation des en-têtes : insérez, modifiez ou supprimez des en-têtes HTTP dans la demande ou la réponse. Par exemple, vous pouvez ajouter un en-tête `True-Client-IP` à chaque requête.
- Redirections ou réécriture d'URL : redirigez les utilisateurs vers d'autres pages en fonction des informations de la demande, ou redirigez toutes les demandes d'un chemin vers un autre.
- Autorisation de demandes : validez des jetons d'autorisations hachés, tels que les jetons web JSON (JWT), en inspectant les en-têtes d'autorisation ou d'autres métadonnées de demandes.

Pour commencer à utiliser CloudFront Functions, consultezPersonnalisez à la périphérie avec CloudFront Functions.

Lambda@Edge est une solution idéale pour les cas d'utilisation suivants :

- Fonctions dont l'exécution peut durer des millisecondes

- Fonctions qui nécessitent un processeur ou une mémoire ajustable
- Fonctions qui dépendent de bibliothèques tierces (y compris le AWS SDK, pour l'intégration avec d'autres Services AWS bibliothèques)
- Fonctions qui nécessitent un accès réseau pour utiliser des services externes pour le traitement
- Fonctions qui nécessitent l’accès au système de fichiers ou au corps des demandes HTTP

Pour démarrer avec Lambda@Edge, consultez Personnalisation en périphérie avec Lambda@Edge.

Pour vous aider à choisir l'option adaptée à votre cas d'utilisation, utilisez le tableau suivant pour comprendre les différences entre CloudFront Functions et Lambda @Edge. Pour en savoir plus sur les différences qui s’appliquent aux méthodes d’assistance à la modification d’origine, consultez Choisissez entre CloudFront Functions et Lambda @Edge.

	CloudFront Fonctions	Lambda@Edge
Langages de programmation	JavaScript (conforme à ECMAScript 5.1)	Node.js et Python
Sources des évènements	• Demande utilisateur • Réponse utilisateur	• Demande utilisateur • Réponse utilisateur • demande à l’origine • Réponse de l’origine
Prend en charge Amazon CloudFront KeyValueStore	Oui CloudFront KeyValueStore ne prend en charge que le JavaScript runtime 2.0	Non
Échelle	Jusqu’à des millions de demandes par seconde	Jusqu'à 10 000 requêtes par seconde et par région
Durée de la fonction	Inférieure à une milliseconde	Jusqu'à 30 secondes (demande et réponse du spectateur)

	CloudFront Fonctions	Lambda@Edge
		Jusqu'à 30 secondes (requête de l'origine et réponse de l'origine)
Taille maximale de la mémoire de la fonction	2 Mo	128 Mo (demande et réponse de l'utilisateur) 10 240 Mo (10 Go) (demande à l'origine et réponse de l'origine) Pour plus d'informations, consultez Quotas sur Lambda@Edge.
Taille maximale du code de fonction et des bibliothèques incluses	10 Ko	50 Mo (demande et réponse de l'utilisateur) 50 Mo (requête de l'origine et réponse de l'origine)
Accès réseau	Non	Oui
Accès au système de fichiers	Non	Oui
Accès au corps de la requête	Non	Oui
Accès à la géolocalisation et aux données de l'appareil	Oui	Non (demande utilisateur et réponse utilisateur) Oui (demande à l'origine et réponse de l'origine)
Peut être créé et testé entièrement dans CloudFront	Oui	Non

	CloudFront Fonctions	Lambda@Edge
Journalisation et métriques des fonctions	Oui	Oui

Personnalisez à la périphérie avec CloudFront Functions

Avec CloudFront Functions, vous pouvez écrire des fonctions légères JavaScript pour des personnalisations CDN à grande échelle et sensibles à la latence. Vos fonctions peuvent manipuler les demandes et les réponses qui circulent CloudFront, effectuer une authentification et une autorisation de base, générer des réponses HTTP en périphérie, etc. L'environnement d'exécution CloudFront Functions offre des temps de démarrage inférieurs à la milliseconde, s'adapte immédiatement pour gérer des millions de requêtes par seconde et est hautement sécurisé. CloudFront Functions est une fonctionnalité native de CloudFront, ce qui signifie que vous pouvez créer, tester et déployer votre code entièrement depuis CloudFront.

Lorsque vous associez une CloudFront fonction à une CloudFront distribution, CloudFront intercepte les demandes et les réponses aux emplacements CloudFront périphériques et les transmet à votre fonction. Vous pouvez appeler CloudFront Functions lorsque les événements suivants se produisent :

- Quand CloudFront reçoit une demande d'un spectateur (demande du spectateur)
- Before CloudFront renvoie la réponse au spectateur (réponse du spectateur)
- Pendant l'établissement de la connexion TLS (demande de connexion) - actuellement disponible pour les connexions TLS mutuelles (mTLS)

Pour plus d'informations sur CloudFront les fonctions, consultez les rubriques suivantes. Pour un didacticiel qui stocke les données dans un magasin de valeurs clés, consultezTutoriel : Création d'une CloudFront fonction incluant des valeurs clés. Après avoir écrit, testé et publié une fonction, vous l'associez à un comportement de cache dans votre distribution — voirAssociation de fonctions à des distributions.

Rubriques

- Tutoriel : Création d'une fonction simple avec CloudFront Functions
- Tutoriel : Création d'une CloudFront fonction incluant des valeurs clés
- Écriture du code de la fonction

- Création de fonctions
- Fonctions de test
- Mise à jour de fonctions
- Publication de fonctions
- Association de fonctions à des distributions
- Amazon CloudFront KeyValueStore

Tutoriel : Création d'une fonction simple avec CloudFront Functions

Ce didacticiel explique comment démarrer avec CloudFront Functions. Vous pouvez créer une fonction simple qui redirige l'utilisateur vers une autre URL et renvoie également un en-tête de réponse personnalisé.

Table des matières

- Conditions préalables
- Créer la fonction
- Vérification de la fonction

Conditions préalables

Pour utiliser CloudFront Functions, vous avez besoin d'une CloudFront distribution. Si vous n'en avez pas, consultez Commencez avec une distribution CloudFront standard.

Créer la fonction

Vous pouvez utiliser la CloudFront console pour créer une fonction simple qui redirige le lecteur vers une autre URL et renvoie également un en-tête de réponse personnalisé.

Pour créer une CloudFront fonction

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Fonctions, puis Créer une fonction.
3. Sur la page Créer une fonction, pour Nom, entrez un nom de fonction tel que*`MyFunctionName`*.
4. (Facultatif) Dans Description, saisissez une description pour la fonction, par exemple, **`Simple test function`**.

5. Pour Runtime, conservez la JavaScript version sélectionnée par défaut.
6. Choisissez Créer une fonction.
7. Copiez le code de fonction suivant. Ce code de fonction redirige l'utilisateur vers une URL différente et renvoie également un en-tête de réponse personnalisé.

```
function handler(event) {
    // NOTE: This example function is for a viewer request event trigger.
    // Choose viewer request for event trigger when you associate this function
 with a distribution.
    var response = {
        statusCode: 302,
        statusDescription: 'Found',
        headers: {
            'cloudfront-functions': { value: 'generated-by-CloudFront-Functions' },
            'location': { value: 'https://aws.amazon.com/cloudfront/' }
        }
    };
    return response;
}
```

8. Dans Code de fonction, collez le code dans l'éditeur de code pour remplacer le code par défaut.
9. Sélectionnez Enregistrer les modifications.
10. (Facultatif) vous pouvez tester la fonction avant de la publier. Ce didacticiel ne décrit pas comment tester une fonction. Pour de plus amples informations, veuillez consulter Fonctions de test.
11. Choisissez l'onglet Publier, puis sélectionnez Publier la fonction. Vous devez publier la fonction avant de pouvoir l'associer à votre CloudFront distribution.
12. Vous pouvez ensuite associer la fonction à une distribution ou à un comportement de cache. Sur la *MyFunctionName* page, choisissez l'onglet Publier.

> **Warning**
>
> Dans les étapes suivantes, choisissez une distribution ou un comportement de cache utilisé pour les tests. N'associez pas cette fonction de test à une distribution ou un comportement de cache utilisé en production.

13. Choisissez Ajouter une association.

14. Dans la boîte de dialogue Association, choisissez une distribution et/ou un comportement de cache. Pour Type d'événement, conservez la valeur par défaut.
15. Choisissez Ajouter une association.

    La table Distributions associées indique la distribution associée.
16. Attendez quelques minutes pour que la distribution associée termine son déploiement. Pour vérifier le statut de la distribution, sélectionnez la distribution dans la table Distributions associées et choisissez Afficher une distribution.

    Lorsque l'état de la distribution est Déployé, vous êtes prêt à vérifier que la fonction fonctionne.

Vérification de la fonction

Après avoir déployé la fonction, vous pouvez vérifier qu'elle fonctionne pour votre distribution.

Pour vérifier la fonction

1. Dans votre navigateur web, accédez au nom de domaine de votre distribution (par exemple, `https://d111111abcdef8.cloudfront.net`).

   La fonction renvoie une redirection vers le navigateur, de sorte que le navigateur ouvre automatiquement `https://aws.amazon.com/cloudfront/`.
2. Dans une fenêtre de ligne de commande, vous pouvez utiliser un outil tel que curl pour envoyer une demande au nom de domaine de votre distribution.

   ```
   curl -v https://d111111abcdef8.cloudfront.net/
   ```

   La réponse affiche la réponse de redirection (`302 Found`) et les en-têtes de réponse personnalisés ajoutés par la fonction. Votre réponse peut ressembler à l'exemple suivant.

   Example

   ```
   curl -v https://d111111abcdef8.cloudfront.net/
   > GET / HTTP/1.1
   > Host: d111111abcdef8.cloudfront.net
   > User-Agent: curl/7.64.1
   > Accept: */*
   >
   < HTTP/1.1 302 Found
   ```

```
< Server: CloudFront
< Date: Tue, 16 Mar 2021 18:50:48 GMT
< Content-Length: 0
< Connection: keep-alive
< Location: https://aws.amazon.com/cloudfront/
< Cloudfront-Functions: generated-by-CloudFront-Functions
< X-Cache: FunctionGeneratedResponse from cloudfront
< Via: 1.1 3035b31bddaf14eded329f8d22cf188c.cloudfront.net (CloudFront)
< X-Amz-Cf-Pop: PHX50-C2
< X-Amz-Cf-Id: ULZdIz6j43uGBlXyob_JctF9x7CCbwpNniiMlmNbmwzH1YWP9FsEHg==
```

Tutoriel : Création d'une CloudFront fonction incluant des valeurs clés

Ce didacticiel explique comment inclure des valeurs clés dans une CloudFront fonction. Les valeurs de clés font partie d'une paire clé-valeur. Vous incluez le nom (provenant de la paire clé-valeur) dans le code de la fonction. Lorsque la fonction s'exécute, CloudFront remplace le nom par la valeur.

Les paires clé-valeur sont des variables stockées dans un magasin de clés-valeurs. Lorsque vous utilisez une clé dans votre fonction (à la place de valeurs codées en dur), votre fonction est plus flexible. Vous pouvez modifier la valeur de la clé sans avoir à déployer de modifications de code. Les paires clé-valeur peuvent également réduire la taille de votre fonction. Pour de plus amples informations, veuillez consulter ???.

Table des matières

- Conditions préalables
- Création du magasin de clés-valeurs
- Ajout des paires clé-valeur au magasin de clés-valeurs
- Association du magasin de clés-valeurs à la fonction
- Test et publication du code de la fonction

Conditions préalables

Si vous découvrez les CloudFront fonctions et le magasin de valeurs clés pour la première fois, nous vous recommandons de suivre le didacticiel dansthe section called “Tutoriel : Création d'une CloudFront fonction simple”.

Une fois ce didacticiel terminé, vous pouvez suivre celui-ci pour étendre la fonction que vous avez créée. Pour ce didacticiel, nous vous recommandons de commencer par créer le magasin de clés-valeurs.

Création du magasin de clés-valeurs

Commencez par créer le magasin de clés-valeurs à utiliser pour votre fonction.

Pour créer le magasin de clés-valeurs

1. Planifiez les paires clé-valeur que vous souhaitez inclure dans la fonction. Notez les noms de clés. Les paires clé-valeur que vous souhaitez utiliser dans une fonction doivent se trouver dans un même magasin de clés-valeurs.
2. Décidez de l'ordre de travail. Il existe deux façons de procéder :
   - Créez un magasin de clés-valeurs et ajoutez-y les paires clé-valeur. Créez (ou modifiez) ensuite la fonction et incorporez les noms des clés.
   - Ou, créez (ou modifiez) la fonction et incorporez les noms des clés que vous voulez utiliser. Créez ensuite un magasin de clés-valeurs et ajoutez les paires clé-valeur.
3. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
4. Dans le volet de navigation, choisissez Functions, puis sélectionnez l'KeyValueStoresonglet.
5. Choisissez Créer KeyValueStore et saisissez les champs suivants :
   - Entrez un nom et une description facultative pour le magasin.
   - Laissez URI S3 vide. Dans ce didacticiel, vous saisirez manuellement les paires clé-valeur.
6. Choisissez Créer. La page de détails du nouveau magasin de clés-valeurs apparaît. Cette page inclut une section Paires clé-valeur qui est actuellement vide.

Ajout des paires clé-valeur au magasin de clés-valeurs

Ensuite, ajoutez manuellement une liste de paires clé-valeur au magasin de clés-valeurs que vous avez créé précédemment.

Pour ajouter des paires clé-valeur au magasin de clés-valeurs

1. Dans la section Paires clé-valeur, choisissez le bouton Ajouter des paires clé-valeur.

2. Choisissez Ajouter une paire et entrez une clé et une valeur. Cochez la case pour confirmer vos modifications et répétez cette étape pour en ajouter d'autres.
3. Lorsque vous avez terminé, choisissez Enregistrer les modifications pour enregistrer les paires clé-valeur dans le magasin de clés-valeurs. Dans la boîte de dialogue de confirmation, choisissez Terminé.

Vous disposez désormais d'un magasin de clés-valeurs qui contient un groupe de paires clé-valeur.

Association du magasin de clés-valeurs à la fonction

Vous avez maintenant créé le magasin de clés-valeurs. Vous avez également créé ou modifié une fonction qui inclut les noms des clés à partir du magasin de clés-valeurs. Vous pouvez maintenant associer le magasin de clés-valeurs et la fonction. Vous créez cette association à partir de la fonction.

Pour associer le magasin de clés-valeurs à la fonction

1. Dans le volet de navigation, choisissez Fonctions. L'onglet Fonctions apparaît en haut, par défaut.
2. Choisissez le nom de la fonction, puis dans la KeyValueStore section Associé, sélectionnez Associer existant KeyValueStore.
3. Sélectionnez le magasin de valeurs clés, puis choisissez Associer KeyValueStore.

> **Note**
>
> Vous pouvez associer un seul magasin de clés-valeurs à chaque fonction.

Test et publication du code de la fonction

Après avoir associé le magasin de clés-valeurs à votre fonction, vous pouvez tester et publier le code de la fonction. Vous devez tester le code de la fonction chaque fois que vous le modifiez, y compris lorsque vous effectuez les opérations suivantes :

- Association d'un magasin de clés-valeurs à la fonction.
- Modification de la fonction et de son magasin de clés-valeurs pour inclure une nouvelle paire clé-valeur.

- Modification de la valeur d'une paire clé-valeur.

Pour tester et publier le code de la fonction

1. Pour en savoir plus sur la façon de tester une fonction, consultez the section called "Fonctions de test". Assurez-vous de choisir de tester la fonction dans la phase `DEVELOPMENT`.
2. Publiez la fonction lorsque vous êtes prêt à l'utiliser (avec les paires clé-valeur nouvelles ou révisées) dans un environnement `LIVE`.

   Lorsque vous publiez, CloudFront copie la version de la fonction de la `DEVELOPMENT` scène vers la scène en direct. La fonction possède le nouveau code et est associée au magasin de clés-valeurs. (Il n'est pas nécessaire de répéter l'association, dans la phase en direct.)

   Pour en savoir plus sur la façon de publier la fonction, consultez the section called "Publication de fonctions".

Écriture du code de la fonction

Vous pouvez utiliser CloudFront Functions pour écrire des fonctions légères dans le cadre de personnalisations JavaScript de CDN à grande échelle et sensibles à la latence. Votre code de fonction peut manipuler les demandes et les réponses qui circulent CloudFront, effectuer une authentification et une autorisation de base, générer des réponses HTTP à la périphérie, etc.

Pour vous aider à écrire du code de fonction pour CloudFront Functions, consultez les rubriques suivantes. Pour des exemples de code, consultez CloudFront Exemples de fonctions pour CloudFront et le référentiel amazon-cloudfront-functions sur. GitHub

Pour utiliser les jetons Web CBOR (CWT) pour l'authentification et l'autorisation basées sur des jetons sur des sites CloudFront périphériques, voir. Support CWT pour les fonctions CloudFront

Rubriques

- Détermination de l'objectif de la fonction
- CloudFront Fonctions, structure de l'événement
- JavaScript fonctionnalités d'exécution pour CloudFront Functions
- Méthodes d'aide pour les magasins de clés-valeurs
- Méthodes d'assistance pour la modification de l'origine
- Méthodes d'assistance pour les propriétés de CloudFront SaaS Manager

- Utilisation asynchrone and await
- Support CWT pour les fonctions CloudFront
- Méthodes d'assistance générales
- Méthodes auxiliaires pour le protocole TLS mutuel

Détermination de l’objectif de la fonction

Avant d'écrire votre code de fonction, déterminez le but de votre fonction. La plupart des CloudFront fonctions de Functions ont l'un des objectifs suivants.

Rubriques

- Modification de la requête HTTP dans un type d'événement de demande de visionnage
- Génération d'une réponse HTTP dans un type d'événement de demande de visionnage
- Modification de la réponse HTTP dans un type d'événement de demande de visionnage
- Valider les connexions mTLS dans un type d'événement de demande de connexion
- Informations connexes

Quel que soit le but de votre fonction, `handler` est le point d'entrée pour n'importe quelle fonction. Il prend un seul argument appelé`event`, qui est transmis à la fonction par CloudFront. `event` est un objet JSON qui contient une représentation de la requête HTTP (et la réponse, si votre fonction modifie la réponse HTTP).

Modification de la requête HTTP dans un type d'événement de demande de visionnage

Votre fonction peut modifier la requête HTTP envoyée CloudFront par le visualiseur (client) et renvoyer la demande modifiée CloudFront pour un traitement continu. Par exemple, votre code de fonction peut normaliser la clé de cache ou modifier les en-têtes de requêtes.

Après avoir créé et publié une fonction qui modifie la demande HTTP, veillez à ajouter une association pour le type d’événement demande de l’utilisateur. Pour plus d’informations, consultez Créer la fonction. Cela permet à la fonction de s'exécuter chaque fois qu' CloudFront elle reçoit une demande d'un visualiseur, avant de vérifier si l'objet demandé se trouve dans le CloudFront cache.

Example Exemple

Le pseudocode suivant montre la structure d'une fonction qui modifie la requête HTTP.

```
function handler(event) {
    var request = event.request;

    // Modify the request object here.

    return request;
}
```

La fonction renvoie l'`request`objet modifié à CloudFront. CloudFrontpoursuit le traitement de la demande renvoyée en vérifiant la CloudFront présence d'un accès au cache et en envoyant la demande à l'origine si nécessaire.

Génération d'une réponse HTTP dans un type d'événement de demande de visionnage

Votre fonction peut générer une réponse HTTP à la périphérie et la renvoyer directement au visualiseur (client) sans vérifier la présence d'une réponse en cache ni aucun autre traitement par CloudFront. Par exemple, votre code de fonction peut rediriger la requête vers une nouvelle URL, ou vérifier l'autorisation et renvoyer une réponse `401` ou `403` à des requêtes non autorisées.

Lorsque vous créez une fonction qui génère une réponse HTTP, veillez à choisir le type d'évènement requête utilisateur. Cela signifie que la fonction s'exécute chaque fois qu' CloudFront elle reçoit une demande d'un utilisateur, avant CloudFront de poursuivre le traitement de la demande.

Example Exemple

Le pseudocode suivant montre la structure d'une fonction qui génère une réponse HTTP.

```
function handler(event) {
    var request = event.request;

    var response = ...; // Create the response object here,
                        // using the request properties if needed.

    return response;
}
```

La fonction renvoie un `response` objet à CloudFront, qui revient CloudFront immédiatement au visualiseur sans vérifier le CloudFront cache ni envoyer de demande à l'origine.

Modification de la réponse HTTP dans un type d'événement de demande de visionnage

Votre fonction peut modifier la réponse HTTP avant de l' CloudFront envoyer au visualiseur (client), que la réponse provienne du CloudFront cache ou de l'origine. Par exemple, votre code de fonction peut ajouter ou modifier des en-têtes de réponse, des codes de statut et le contenu du corps.

Lorsque vous créez une fonction qui modifie la réponse HTTP, veillez à choisir le type d'évènement réponse utilisateur. Cela signifie que la fonction s'exécute avant de CloudFront renvoyer une réponse au visualiseur, que la réponse provienne du CloudFront cache ou de l'origine.

Example Exemple

Le pseudocode suivant montre la structure d'une fonction qui modifie la réponse HTTP.

```
function handler(event) {
    var request = event.request;
    var response = event.response;

    // Modify the response object here,
    // using the request properties if needed.

    return response;
}
```

La fonction renvoie l'`response`objet modifié à CloudFront, qui revient CloudFront immédiatement au visualiseur.

Valider les connexions mTLS dans un type d'événement de demande de connexion

Les fonctions de connexion sont un type de CloudFront fonctions qui s'exécutent pendant les connexions TLS pour fournir une logique de validation et d'authentification personnalisée. Les fonctions de connexion sont actuellement disponibles pour les connexions TLS mutuelles (MTLS), où vous pouvez valider les certificats clients et implémenter une logique d'authentification personnalisée au-delà de la validation standard des certificats. Les fonctions de connexion s'exécutent pendant le processus de prise de contact TLS et peuvent autoriser ou refuser des connexions en fonction des propriétés des certificats, des adresses IP des clients ou d'autres critères.

Après avoir créé et publié une fonction de connexion, assurez-vous d'ajouter une association pour le type d'événement de demande de connexion avec une TLS-enabled distribution m. Cela permet à la fonction de s'exécuter chaque fois qu'un client tente d'établir une connexion mTLS avec CloudFront.

Example

Le pseudocode suivant montre la structure d'une fonction de connexion :

```
function connectionHandler(connection) {
    // Validate certificate and connection properties here.

    if (/* validation passes */) {
        connection.allow();
    } else {
        connection.deny();
    }
}
```

La fonction utilise des méthodes d'assistance pour déterminer s'il convient d'autoriser ou de refuser la connexion. Contrairement aux fonctions de demande et de réponse de l'utilisateur, les fonctions de connexion ne peuvent pas modifier les requêtes ou les réponses HTTP.

Informations connexes

Pour plus d'informations sur l'utilisation des CloudFront fonctions, consultez les rubriques suivantes :

- Structure d’évènements
- JavaScript fonctionnalités d'exécution
- CloudFront Exemples de fonctions
- Restrictions sur les fonctions périphériques

CloudFront Fonctions, structure de l'événement

CloudFront Functions transmet un `event` objet au code de votre fonction en tant qu'entrée lorsqu'il exécute la fonction. Lorsque vous testez une fonction, vous créez l'objet `event` et le transférez à votre fonction. Lorsque vous créez un objet `event` pour tester une fonction, vous pouvez omettre les champs `distributionDomainName`, `distributionId` et `requestId` de l'objet `context`. Assurez-vous que les noms des en-têtes sont en minuscules, ce qui est toujours le cas pour l'`event`objet que CloudFront Functions transmet à votre fonction en production.

La section suivante présente une vue d'ensemble de la structure de cet objet d'évènement.

```
{
```

```
    "version": "1.0",
    "context": {
        <context object>
    },
    "viewer": {
        <viewer object>
    },
    "request": {
        <request object>
    },
    "response": {
        <response object>
    }
}
```

Pour plus d'informations, consultez les rubriques suivantes :

Rubriques

- Champ Version
- Objet Contexte
- Structure des événements de connexion
- Objet Utilisateur
- Objet Requête
- Objet Réponse
- Code de statut et corps
- Structure d'une chaîne de requête, d'un en-tête ou d'un cookie
- Exemple d'objet de réponse
- Exemple d'objet d'événement

Champ Version

Le `version` champ contient une chaîne qui spécifie la version de l'objet d'événement CloudFront Functions. La version actuelle est `1.0`.

Objet Contexte

L'objet `context` contient des informations contextuelles sur l'évènement. Il inclut les champs suivants :

`distributionDomainName`

Le nom CloudFront de domaine (par exemple, d111111abcdef8.cloudfront.net) de la distribution standard associée à l'événement.

Le champ `distributionDomainName` n'apparaît que lorsque votre fonction est invoquée pour les distributions standard.

`endpoint`

Le nom CloudFront de domaine (par exemple, d111111abcdef8.cloudfront.net) du groupe de connexions associé à l'événement.

Le champ `endpoint` n'apparaît que lorsque votre fonction est invoquée pour les distributions multi-locataires.

`distributionId`

ID de la distribution (par exemple EDFDVBD6EXAMPLE) associée à l'événement.

`eventType`

Le type d'évènement, `viewer-request` ou `viewer-response`.

`requestId`

Chaîne qui identifie de manière unique une CloudFront demande (et sa réponse associée).

Structure des événements de connexion

Les fonctions de connexion reçoivent une structure d'événements différente de celle des fonctions d'affichage. Pour des informations détaillées sur la structure des événements de connexion et le format de réponse, consultezAssocier une fonction CloudFront de connexion.

Objet Utilisateur

L'objet `viewer` comporte un champ `ip` dont la valeur est l'adresse IP de l'utilisateur (client) qui a envoyé la requête. Si la requête utilisateur a été envoyée via un proxy HTTP ou un équilibreur de charge, la valeur correspond à l'adresse IP du proxy ou de l'équilibreur de charge.

Objet Requête

L'`request`objet contient une représentation d'une requête HTTP entre le visualiseur et le protocole HTTP. CloudFront Dans l'`event`objet transmis à votre fonction, l'`request`objet représente la demande réelle qui CloudFront a été reçue de la part du spectateur.

Si votre code de fonction renvoie un `request` objet à CloudFront, il doit utiliser la même structure.

L'objet `request` comporte les champs suivants :

`method`

Méthode HTTP de la demande. Si votre code de fonction renvoie une `request`, il ne peut pas modifier ce champ. Il s'agit du seul champ en lecture seule de l'objet `request`.

`uri`

Chemin d’accès relatif de l’objet demandé.

> **Note**
>
> Si votre fonction modifie la valeur `uri`, les règles suivantes s’appliquent :
>
> - La nouvelle valeur `uri` doit commencer par une barre oblique (`/`).
> - Lorsqu'une fonction modifie la valeur `uri`, elle change l'objet que l'utilisateur demande.
> - Quand une fonction modifie la valeur `uri`, elle ne modifie pas le comportement de cache pour la demande ni l'origine vers laquelle la demande d'origine est envoyée.

`querystring`

Objet qui représente la chaîne de requête dans la requête. Si la demande n'inclut pas de chaîne de requête, l'objet `request` inclut néanmoins un objet `querystring` vide.

L'objet `querystring` comporte un champ pour chaque paramètre de chaîne de requête dans la requête.

`headers`

Objet qui représente les en-têtes HTTP dans la requête. Si la requête contient des en-têtes `Cookie`, ces derniers ne font pas partie de l'objet `headers`. Les cookies sont représentés séparément dans l'objet `cookies`.

L'objet `headers` comporte un champ pour chaque en-tête de la requête. Les noms d'en-tête sont convertis ASCII-lowercase dans l'objet d'événement, et les noms d'en-tête doivent l'être ASCII-lowercase lorsqu'ils sont ajoutés par le code de votre fonction. Lorsque CloudFront Functions reconvertit l'objet d'événement en requête HTTP, la première lettre de chaque mot des noms d'en-tête est mise en majuscule, s'il s'agit d'un ASCII-letter. CloudFront Functions n'applique aucune

modification aux symboles non ASCII dans les noms d'en-tête. Par exemple, `TÈst-header` deviendra `tÈst-header` à l'intérieur de la fonction. Le symbole non ASCII È est inchangé.

Les mots sont séparés par un trait d'union (`-`). Par exemple, si le code de votre fonction ajoute un en-tête nommé`example-header-name`, CloudFront convertissez-le en `Example-Header-Name` dans la requête HTTP.

`cookies`

Objet qui représente les cookies dans la requête (en-têtes `Cookie`).

L'objet `cookies` comporte un champ pour chaque cookie dans la requête.

Pour plus d'informations sur la structure des chaînes de requêtes, des en-têtes et des cookies, consultez Structure d'une chaîne de requête, d'un en-tête ou d'un cookie.

Pour un exemple d'objet `event`, consultez Exemple d'objet d'événement.

Objet Réponse

L'`response`objet contient une représentation d'une réponse CloudFront-to-viewer HTTP. Dans l'`event`objet transmis à votre fonction, l'`response`objet représente la réponse CloudFront réelle à une demande de l'utilisateur.

Si votre code de fonction renvoie un objet `response`, il doit utiliser cette même structure.

L'objet `response` comporte les champs suivants :

`statusCode`

Code de statut HTTP de la réponse. Cette valeur est un entier, pas une chaîne.

Votre fonction peut générer ou modifier le `statusCode`.

`statusDescription`

Description de l'état HTTP de la réponse. Si votre code de fonction génère une réponse, ce champ est facultatif.

`headers`

Objet qui représente les en-têtes HTTP dans la réponse. Si la réponse contient des en-têtes `Set-Cookie`, ces derniers ne font pas partie de l'objet `headers`. Les cookies sont représentés séparément dans l'objet `cookies`.

L'objet `headers` comporte un champ pour chaque en-tête de la réponse. Les noms des en-têtes sont convertis en minuscules dans l'objet d'événement, et les noms des en-têtes doivent être en minuscules lorsqu'ils sont ajoutés par votre code de fonction. Lorsque CloudFront Functions reconvertit l'objet d'événement en réponse HTTP, la première lettre de chaque mot des noms d'en-tête est mise en majuscule. Les mots sont séparés par un trait d'union (`-`). Par exemple, si le code de votre fonction ajoute un en-tête nommé`example-header-name`, CloudFront convertissez-le en `Example-Header-Name` dans la réponse HTTP.

`cookies`

Objet qui représente les cookies dans la réponse (en-têtes `Set-Cookie`).

L'objet `cookies` comporte un champ pour chaque cookie dans la réponse.

`body`

L'ajout du champ `body` est facultatif et il ne sera pas présent dans l'objet `response` à moins que vous ne le spécifiiez dans votre fonction. Votre fonction n'a pas accès au corps d'origine renvoyé par le CloudFront cache ou l'origine. Si vous ne spécifiez pas le `body` champ dans votre fonction de réponse du spectateur, le corps d'origine renvoyé par le CloudFront cache ou l'origine est renvoyé au visualiseur.

Si vous CloudFront souhaitez renvoyer un corps personnalisé au visualiseur, spécifiez le contenu du corps dans le `data` champ et le codage du corps dans le `encoding` champ. Vous pouvez spécifier le codage sous forme de texte brut (`"encoding": "text"`) ou de Base64-encoded contenu (`"encoding": "base64"`).

Comme raccourci, vous pouvez également spécifier le contenu du corps directement dans le champ `body` (`"body": "<specify the body content here>"`). Dans ce cas, omettez les `encoding` champs `data` et. CloudFront traite le corps comme du texte brut dans ce cas.

`encoding`

Codage du contenu de `body` (champ `data`). Les seuls encodages valides sont `text` et `base64`.

Si vous spécifiez `encoding` as `base64` mais que le corps n'est pas valide en base64, CloudFront renvoie une erreur.

`data`

Contenu de `body`.

Pour plus d'informations sur les codes de statut modifiés et le contenu du corps, consultez Code de statut et corps.

Pour plus d'informations sur la structure des en-têtes et des cookies, consultez Structure d'une chaîne de requête, d'un en-tête ou d'un cookie.

Pour un exemple d'objet `response`, consultez Exemple d'objet de réponse.

Code de statut et corps

Grâce à CloudFront Functions, vous pouvez mettre à jour le code d'état de la réponse de l'utilisateur, remplacer l'intégralité du corps de la réponse par un nouveau ou supprimer le corps de la réponse. Certains scénarios courants de mise à jour de la réponse de l'utilisateur après avoir évalué certains aspects de la réponse depuis le CloudFront cache ou l'origine sont les suivants :

- Modification du statut pour définir un code de statut HTTP 200 et création d'un contenu de corps statique à renvoyer à l'utilisateur.
- Modification du statut pour définir un code de statut HTTP 301 ou 302 afin de rediriger l'utilisateur vers un autre site Web.
- Décider de diffuser ou de supprimer le corps de la réponse d'utilisateur.

> **Note**
>
> Si l'origine renvoie une erreur HTTP de 400 ou plus, la CloudFront fonction ne sera pas exécutée. Pour plus d'informations, consultez Restrictions sur toutes les fonctions périphériques.

Lorsque vous utilisez la réponse HTTP, CloudFront Functions n'a pas accès au corps de la réponse. Vous pouvez remplacer le contenu du corps en lui attribuant la valeur souhaitée, ou supprimer le corps en définissant une valeur vide. Si vous ne mettez pas à jour le champ du corps dans votre fonction, le corps d'origine renvoyé par le CloudFront cache ou l'origine est renvoyé au visualiseur.

> **Tip**
>
> Lorsque vous utilisez CloudFront Functions pour remplacer un corps, veillez à aligner les en-têtes correspondants, tels que`content-encoding`, ou `content-type``content-length`, sur le nouveau contenu du corps.

Par exemple, si l' CloudFront origine ou le cache sont renvoyés `content-encoding: gzip` mais que la fonction de réponse de l'utilisateur définit un corps en texte brut, la fonction doit également modifier `content-type` les en-têtes `content-encoding` et en conséquence.

Si votre CloudFront fonction est configurée pour renvoyer une erreur HTTP de 400 ou plus, votre utilisateur ne verra pas la page d'erreur personnalisée que vous avez spécifiée pour le même code d'état.

Structure d'une chaîne de requête, d'un en-tête ou d'un cookie

Les chaînes de requête, les en-têtes et les cookies partagent la même structure. Les chaînes de requête peuvent apparaître dans les demandes. Les en-têtes apparaissent dans les demandes et les réponses. Les cookies apparaissent dans les demandes et les réponses.

Chaque chaîne de requête, en-tête ou cookie est un champ unique au sein de l'objet parent `querystring`, `headers` ou `cookies`. Le nom du champ est le nom de la chaîne de requête, de l'en-tête ou du cookie. Chaque champ comporte une propriété `value` avec la valeur de la chaîne de requête, de l'en-tête ou du cookie.

Table des matières

- Valeurs de chaînes de requête ou objets de chaîne de requête
- Considérations spéciales pour les en-têtes
- Chaînes de requête, en-têtes et cookies dupliqués (tableau MultiValue)
- Attributs de cookies

Valeurs de chaînes de requête ou objets de chaîne de requête

Une fonction peut renvoyer une valeur de chaîne de requête en plus d'un objet de chaîne de requête. La valeur de chaîne de requête peut être utilisée pour organiser les paramètres de chaîne de requête dans n'importe quel ordre personnalisé.

Example Exemple

Pour modifier une chaîne de requête dans le code d’une fonction, utilisez un code analogue au suivant.

```
var request = event.request;
```

```
request.querystring =
 'ID=42&Exp=1619740800&TTL=1440&NoValue=&querymv=val1&querymv=val2,val3';
```

Considérations spéciales pour les en-têtes

Pour les en-têtes uniquement, les noms des en-têtes sont convertis en minuscules dans l'objet d'événement, et les noms des en-têtes doivent être en minuscules lorsqu'ils sont ajoutés par votre code de fonction. Lorsque CloudFront Functions reconvertit l'objet d'événement en une requête ou une réponse HTTP, la première lettre de chaque mot des noms d'en-tête est mise en majuscule. Les mots sont séparés par un trait d'union (`-`). Par exemple, si le code de votre fonction ajoute un en-tête nommé`example-header-name`, CloudFront convertissez-le en `Example-Header-Name` dans la requête ou la réponse HTTP.

Example Exemple

Examinez l'en-tête `Host` suivant dans une demande HTTP.

```
Host: video.example.com
```

Cet en-tête est représenté comme suit dans l'objet `request` :

```
"headers": {
    "host": {
        "value": "video.example.com"
    }
}
```

Pour accéder à l'en-tête `Host` dans votre code de fonction, utilisez le code comme suit :

```
var request = event.request;
var host = request.headers.host.value;
```

Pour ajouter ou modifier un en-tête dans votre code de fonction, utilisez le code suivant (ce code ajoute un en-tête nommé `X-Custom-Header` avec la valeur `example value`) :

```
var request = event.request;
request.headers['x-custom-header'] = {value: 'example value'};
```

Chaînes de requête, en-têtes et cookies dupliqués (tableau **`MultiValue`**)

Une requête ou une réponse HTTP peut contenir plusieurs chaînes de requêtes, en-têtes ou cookies portant le même nom. Dans ce cas, les chaînes de requêtes, les en-têtes ou les cookies en double sont regroupés dans un champ de l'objet `request` ou `response`, mais ce champ comporte une propriété supplémentaire nommée `multiValue`. La propriété `multiValue` contient un tableau avec les valeurs de chacun des en-têtes, cookies ou chaînes de requêtes dupliqués.

Example Exemple

Imaginons une requête HTTP qui inclut les en-têtes `Accept` suivants.

```
Accept: application/json
Accept: application/xml
Accept: text/html
```

Ces en-têtes sont représentés comme suit dans l'objet `request`.

```
"headers": {
    "accept": {
        "value": "application/json",
        "multiValue": [
            {
                "value": "application/json"
            },
            {
                "value": "application/xml"
            },
            {
                "value": "text/html"
            }
        ]
    }
}
```

> **Note**
>
> La première valeur d'en-tête (dans ce cas, `application/json`) est répétée dans les propriétés `value` et `multiValue`. Cela vous permet d'accéder à toutes les valeurs en faisant une boucle dans le tableau `multiValue`.

Si le code de votre fonction modifie une chaîne de requête, un en-tête ou un cookie contenant un `multiValue` tableau, CloudFront Functions applique les règles suivantes pour appliquer les modifications :

1. Si le tableau `multiValue` existe et comporte des modifications, ces dernières sont appliquées. Le premier élément de la propriété `value` est ignoré.
2. Sinon, toute modification apportée à la propriété `value` est appliquée, et les valeurs suivantes (si elles existent) restent inchangées.

La propriété `multiValue` est utilisée uniquement lorsque la requête ou la réponse HTTP contient des chaînes de requêtes, des en-têtes ou des cookies en double portant le même nom, comme indiqué dans l'exemple précédent. Toutefois, s'il existe plusieurs valeurs dans un seul en-tête, cookie ou chaîne de requête, la propriété `multiValue` n'est pas utilisée.

Example Exemple

Prenons l’exemple d’une demande avec un en-tête `Accept` contenant trois valeurs.

```
Accept: application/json, application/xml, text/html
```

Cet en-tête est représenté comme suit dans l’objet `request`.

```
"headers": {
    "accept": {
        "value": "application/json, application/xml, text/html"
    }
}
```

Attributs de cookies

Dans un en-tête `Set-Cookie` d'une réponse HTTP, l'en-tête contient la paire nom-valeur du cookie et éventuellement un ensemble d'attributs séparés par des points-virgules.

Example Exemple

```
Set-Cookie: cookie1=val1; Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT
```

Dans l'objet `response`, ces attributs sont représentés dans la propriété `attributes` du champ cookie. Par exemple, l'en-tête `Set-Cookie` précédent est représenté comme suit :

```
"cookie1": {
    "value": "val1",
    "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT"
}
```

Exemple d'objet de réponse

L'exemple suivant montre un objet `response` (la sortie d'une fonction de réponse d'utilisateur) dans lequel le corps a été remplacé par une fonction de réponse d'utilisateur.

```
{
  "response": {
    "statusCode": 200,
    "statusDescription": "OK",
    "headers": {
      "date": {
        "value": "Mon, 04 Apr 2021 18:57:56 GMT"
      },
      "server": {
        "value": "gunicorn/19.9.0"
      },
      "access-control-allow-origin": {
        "value": "*"
      },
      "access-control-allow-credentials": {
        "value": "true"
      },
      "content-type": {
        "value": "text/html"
      },
      "content-length": {
        "value": "86"
      }
    },
    "cookies": {
      "ID": {
        "value": "id1234",
        "attributes": "Expires=Wed, 05 Apr 2021 07:28:00 GMT"
      },
```

```
      "Cookie1": {
        "value": "val1",
        "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT",
        "multiValue": [
          {
            "value": "val1",
            "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr 2021
 07:28:00 GMT"
          },
          {
            "value": "val2",
            "attributes": "Path=/cat; Domain=example.com; Expires=Wed, 10 Jan 2021
 07:28:00 GMT"
          }
        ]
      }
    },

    // Adding the body field is optional and it will not be present in the response
 object
    // unless you specify it in your function.
    // Your function does not have access to the original body returned by the
 CloudFront
    // cache or origin.
    // If you don't specify the body field in your viewer response function, the
 original
    // body returned by the CloudFront cache or origin is returned to viewer.

     "body": {
      "encoding": "text",
      "data": "<!DOCTYPE html><html><body><p>Here is your custom content.</p></body></
html>"
    }
  }
}
```

Exemple d'objet d'événement

L'exemple suivant illustre un objet `event` complet. Il s'agit d'un exemple d'invocation pour une distribution standard, et non pour une distribution multi-locataires. Pour les distributions multi-locataires, le `endpoint` champ est utilisé à la place de `distributionDomainName` La valeur de

`endpoint` est le nom de CloudFront domaine (par exemple, d111111abcdef8.cloudfront.net) du groupe de connexions associé à l'événement.

> **Note**
>
> L'objet `event` représente l'entrée de votre fonction. Votre fonction renvoie uniquement l'objet `request` ou `response`, et non l'objet `event` complet.

```
{
    "version": "1.0",
    "context": {
        "distributionDomainName": "d111111abcdef8.cloudfront.net",
        "distributionId": "EDFDVBD6EXAMPLE",
        "eventType": "viewer-response",
        "requestId": "EXAMPLEntjQpEXAMPLE_SG5Z-EXAMPLEPmPfEXAMPLEu3EqEXAMPLE=="
    },
    "viewer": {"ip": "198.51.100.11"},
    "request": {
        "method": "GET",
        "uri": "/media/index.mpd",
        "querystring": {
            "ID": {"value": "42"},
            "Exp": {"value": "1619740800"},
            "TTL": {"value": "1440"},
            "NoValue": {"value": ""},
            "querymv": {
                "value": "val1",
                "multiValue": [
                    {"value": "val1"},
                    {"value": "val2,val3"}
                ]
            }
        },
        "headers": {
            "host": {"value": "video.example.com"},
            "user-agent": {"value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0)
 Gecko/20100101 Firefox/83.0"},
            "accept": {
                "value": "application/json",
                "multiValue": [
                    {"value": "application/json"},
```

```
                    {"value": "application/xml"},
                    {"value": "text/html"}
                ]
            },
            "accept-language": {"value": "en-GB,en;q=0.5"},
            "accept-encoding": {"value": "gzip, deflate, br"},
            "origin": {"value": "https://website.example.com"},
            "referer": {"value": "https://website.example.com/videos/12345678?
action=play"},
            "cloudfront-viewer-country": {"value": "GB"}
        },
        "cookies": {
            "Cookie1": {"value": "value1"},
            "Cookie2": {"value": "value2"},
            "cookie_consent": {"value": "true"},
            "cookiemv": {
                "value": "value3",
                "multiValue": [
                    {"value": "value3"},
                    {"value": "value4"}
                ]
            }
        }
    },
    "response": {
        "statusCode": 200,
        "statusDescription": "OK",
        "headers": {
            "date": {"value": "Mon, 04 Apr 2021 18:57:56 GMT"},
            "server": {"value": "gunicorn/19.9.0"},
            "access-control-allow-origin": {"value": "*"},
            "access-control-allow-credentials": {"value": "true"},
            "content-type": {"value": "application/json"},
            "content-length": {"value": "701"}
        },
        "cookies": {
            "ID": {
                "value": "id1234",
                "attributes": "Expires=Wed, 05 Apr 2021 07:28:00 GMT"
            },
            "Cookie1": {
                "value": "val1",
                "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed, 05 Apr
 2021 07:28:00 GMT",
```

```
                "multiValue": [
                    {
                        "value": "val1",
                        "attributes": "Secure; Path=/; Domain=example.com; Expires=Wed,
 05 Apr 2021 07:28:00 GMT"
                    },
                    {
                        "value": "val2",
                        "attributes": "Path=/cat; Domain=example.com; Expires=Wed, 10
 Jan 2021 07:28:00 GMT"
                    }
                ]
            }
        }
    }
}
```

JavaScript fonctionnalités d'exécution pour CloudFront Functions

L'environnement JavaScript d'exécution CloudFront Functions est compatible avec ECMAScript (ES) version 5.1 et prend également en charge certaines fonctionnalités des versions ES 6 à 12.

Pour la plupart des up-to-date fonctionnalités, nous vous recommandons JavaScript d'utiliser Runtime 2.0.

Les fonctionnalités JavaScript d'exécution 2.0 présentent les modifications suivantes par rapport à la version 1.0 :

- Les méthodes du module Buffer sont disponibles
- Les méthodes de prototype de chaîne non standard suivantes ne sont pas disponibles :
  - `String.prototype.bytesFrom()`
  - `String.prototype.fromBytes()`
  - `String.prototype.fromUTF8()`
  - `String.prototype.toBytes()`
  - `String.prototype.toUTF8()`
- Voici les nouveautés du module cryptographique :
  - `hash.digest()` : le type de retour est remplacé par `Buffer` si aucun encodage n'est fourni
  - `hmac.digest()` : le type de retour est remplacé par `Buffer` si aucun encodage n'est fourni

- Pour plus d'informations sur les nouvelles fonctionnalités supplémentaires, consultez JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions.

Rubriques

- JavaScript fonctionnalités de Runtime 1.0 pour CloudFront Functions
- JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions

JavaScript fonctionnalités de Runtime 1.0 pour CloudFront Functions

L'environnement JavaScript d'exécution CloudFront Functions est compatible avec ECMAScript (ES) version 5.1 et prend également en charge certaines fonctionnalités des versions ES 6 à 9. Il fournit également des méthodes non standard qui ne font pas partie des spécifications ES.

Les rubriques suivantes répertorient toutes les fonctions de langages prises en charge.

Rubriques

- Fonctions de base
- Objets primitifs
- Objets intégrés
- Types d'erreurs
- Globals
- Modules intégrés
- Fonctions limitées

Fonctions de base

Les fonctions de base suivantes d'ES sont prises en charge.

Types

Tous les types ES 5.1 sont pris en charge, notamment les valeurs booléennes, les nombres, les chaînes, les objets, les tableaux, les fonctions, les constructeurs de fonctions et les expressions régulières.

Opérateurs

Tous les opérateurs ES 5.1 sont pris en charge.

L'opérateur d'exponentiation ES 7 (`**`) est pris en charge.

Instructions

> **Note**
>
> Les instructions `const` et `let` ne sont pas prises en charge.

Les instructions ES 5.1 suivantes sont prises en charge :

- `break`
- `catch`
- `continue`
- `do-while`
- `else`
- `finally`
- `for`
- `for-in`
- `if`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`
- Instructions étiquetées

Littéraux

Les littéraux de modèles ES 6 sont pris en charge : chaînes multiligne, interpolation d'expression et modèles d'imbrication.

Fonctions

Toutes les fonctions ES 5.1 sont prises en charge.

Les fonctions de flèche ES 6 ainsi que la syntaxe des paramètres du reste ES 6 sont prises en charge.

Unicode

Le texte source et les littéraux de chaînes peuvent contenir des caractères Unicode. Les séquences d'échappement de points de code Unicode de six caractères (par exemple `\uXXXX`) sont également prises en charge.

Mode strict

Les fonctions opèrent en mode strict par défaut. Vous n'avez donc pas besoin d'ajouter une instruction `use strict` dans votre code de fonction. Elles ne peuvent pas être modifiées.

Objets primitifs

Les objets primitifs suivants d'ES sont pris en charge.

Objet

Les méthodes ES 5.1 suivantes sur les objets sont prises en charge :

- `create` (sans liste de propriétés)
- `defineProperties`
- `defineProperty`
- `freeze`
- `getOwnPropertyDescriptor`
- `getOwnPropertyNames`
- `getPrototypeOf`
- `hasOwnProperty`
- `isExtensible`
- `isFrozen`
- `prototype.isPrototypeOf`
- `isSealed`
- `keys`
- `preventExtensions`
- `prototype.propertyIsEnumerable`

- `seal`
- `prototype.toString`
- `prototype.valueOf`

Les méthodes ES 6 suivantes sur les objets sont prises en charge :

- `assign`
- `is`
- `prototype.setPrototypeOf`

Les méthodes ES 8 suivantes sur les objets sont prises en charge :

- `entries`
- `values`

String

Les méthodes ES 5.1 suivantes sur les chaînes sont prises en charge :

- `fromCharCode`
- `prototype.charAt`
- `prototype.concat`
- `prototype.indexOf`
- `prototype.lastIndexOf`
- `prototype.match`
- `prototype.replace`
- `prototype.search`
- `prototype.slice`
- `prototype.split`
- `prototype.substr`
- `prototype.substring`
- `prototype.toLowerCase`
- `prototype.trim`
- `prototype.toUpperCase`

Les méthodes ES 6 suivantes sur les chaînes sont prises en charge :

- `fromCodePoint`

- `prototype.codePointAt`
- `prototype.endsWith`
- `prototype.includes`
- `prototype.repeat`
- `prototype.startsWith`

Les méthodes ES 8 suivantes sur les chaînes sont prises en charge :

- `prototype.padStart`
- `prototype.padEnd`

Les méthodes ES 9 suivantes sur les chaînes sont prises en charge :

- `prototype.trimStart`
- `prototype.trimEnd`

Les méthodes non standard suivantes sur les chaînes sont prises en charge :

- `prototype.bytesFrom(`*`array | string, encoding`*`)`

  Crée une chaîne d'octets à partir d'un tableau d'octets ou d'une chaîne encodée. Les options d'encodage de chaînes sont `hex`, `base64` et `base64url`.

- `prototype.fromBytes(`*`start`*`[, `*`end`*`])`

  Crée une chaîne Unicode à partir d'une chaîne d'octets où chaque octet est remplacé par le point de code Unicode correspondant.

- `prototype.fromUTF8(`*`start`*`[, `*`end`*`])`

  Crée une chaîne Unicode à partir d'une chaîne d'octets encodée en UTF-8. Si l'encodage est incorrect, il renvoie `null`.

- `prototype.toBytes(start[, end])`

  Crée une chaîne d'octets à partir d'une chaîne Unicode. Tous les caractères doivent être dans la plage [0,255]. Dans le cas contraire, `null` est renvoyé.

- `prototype.toUTF8(start[, `*`end`*`])`

  Crée une chaîne d'octets encodée en UTF-8 à partir d'une chaîne Unicode.

Nombre

Toutes les méthodes ES 5.1 sur les nombres sont prises en charge.

Les méthodes ES 6 suivantes sur les nombres sont prises en charge :

- `isFinite`
- `isInteger`
- `isNaN`
- `isSafeInteger`
- `parseFloat`
- `parseInt`
- `prototype.toExponential`
- `prototype.toFixed`
- `prototype.toPrecision`
- `EPSILON`
- `MAX_SAFE_INTEGER`
- `MAX_VALUE`
- `MIN_SAFE_INTEGER`
- `MIN_VALUE`
- `NEGATIVE_INFINITY`
- `NaN`
- `POSITIVE_INFINITY`

Objets intégrés

Les objets intégrés suivants d'ES sont pris en charge.

Mathématiques

Toutes les méthodes mathématiques ES 5.1 sont prises en charge.

> **Note**
>
> Dans l'environnement d'exécution de CloudFront Functions, l'`Math.random()`implémentation utilise `arc4random` OpenBSD prédéfini avec l'horodatage de l'exécution de la fonction.

Les méthodes mathématiques ES 6 suivantes sont prises en charge :

- `acosh`
- `asinh`
- `atanh`
- `cbrt`
- `clz32`
- `cosh`
- `expm1`
- `fround`
- `hypot`
- `imul`
- `log10`
- `log1p`
- `log2`
- `sign`
- `sinh`
- `tanh`
- `trunc`
- `E`
- `LN10`
- `LN2`
- `LOG10E`
- `LOG2E`
- `PI`
- `SQRT1_2`
- `SQRT2`

Date

Toutes les fonctions `Date` ES 5.1 sont prises en charge.

> **Note**
>
> Pour des raisons de sécurité, `Date` renvoie toujours la même valeur (l'heure de début de la fonction) pendant la durée de vie d'une même exécution de la fonction. Pour plus d'informations, consultez Fonctions limitées.

Fonction

Les méthodes `apply`, `bind` et `call` sont prises en charge.

Les constructeurs de fonctions ne sont pas pris en charge.

Expressions régulières

Toutes les fonctions d'expression régulière ES 5.1 sont prises en charge. Le langage d'expression régulière est compatible Perl. Les groupes de capture nommés ES 9 sont pris en charge.

JSON

Toutes les fonctions JSON ES 5.1 sont prises en charge, notamment `parse` et `stringify`.

Array

Les méthodes ES 5.1 suivantes sur les tableaux sont prises en charge :

- `isArray`
- `prototype.concat`
- `prototype.every`
- `prototype.filter`
- `prototype.forEach`
- `prototype.indexOf`
- `prototype.join`
- `prototype.lastIndexOf`
- `prototype.map`
- `prototype.pop`
- `prototype.push`
- `prototype.reduce`

- `prototype.reduceRight`
- `prototype.reverse`
- `prototype.shift`
- `prototype.slice`
- `prototype.some`
- `prototype.sort`
- `prototype.splice`
- `prototype.unshift`

Les méthodes ES 6 suivantes sur les tableaux sont prises en charge :

- `of`
- `prototype.copyWithin`
- `prototype.fill`
- `prototype.find`
- `prototype.findIndex`

Les méthodes ES 7 suivantes sur les tableaux sont prises en charge :

- `prototype.includes`

Tableaux typés

Les tableaux typés ES 6 suivants sont pris en charge :

- `Int8Array`
- `Uint8Array`
- `Uint8ClampedArray`
- `Int16Array`
- `Uint16Array`
- `Int32Array`
- `Uint32Array`
- `Float32Array`
- `Float64Array`
- `prototype.copyWithin`

- `prototype.fill`
- `prototype.join`
- `prototype.set`
- `prototype.slice`
- `prototype.subarray`
- `prototype.toString`

ArrayBuffer

Les méthodes suivantes sur `ArrayBuffer` sont prises en charge :

- `prototype.isView`
- `prototype.slice`

Promesse

Les méthodes suivantes sur les promesses sont prises en charge :

- `reject`
- `resolve`
- `prototype.catch`
- `prototype.finally`
- `prototype.then`

Cryptographie

Le module cryptographique fournit des aides standard en matière de hachage et de code d'authentification de message basé sur le hachage (HMAC). Vous pouvez charger le module en utilisant `require('crypto')`. Le module fournit les méthodes suivantes, qui se comportent exactement comme leurs homologues Node.js :

- `createHash(`*`algorithm`*`)`
- `hash.update(`*`data`*`)`
- `hash.digest([`*`encoding`*`])`
- `createHmac(`*`algorithm, secret key`*`)`
- `hmac.update(`*`data`*`)`
- `hmac.digest([`*`encoding`*`])`

Pour plus d'informations, consultez Cryptographie (hachage et HMAC) dans la section Modules intégrés.

Console

Il s'agit d'un objet d'aide pour le débogage. Il ne prend en charge que la méthode `log()`, pour enregistrer les messages de journaux.

> **Note**
>
> CloudFront Les fonctions ne prennent pas en charge la syntaxe des virgules, telle que`console.log('a', 'b')`. Utilisez plutôt le format `console.log('a' + ' ' + 'b')`.

Types d'erreurs

Les objets d'erreurs suivants sont pris en charge :

- `Error`
- `EvalError`
- `InternalError`
- `MemoryError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Globals

L'objet `globalThis` est pris en charge.

Les fonctions globales ES 5.1 suivantes sont prises en charge :

- `decodeURI`
- `decodeURIComponent`
- `encodeURI`

- `encodeURIComponent`
- `isFinite`
- `isNaN`
- `parseFloat`
- `parseInt`

Les constantes globales suivantes sont prises en charge :

- `NaN`
- `Infinity`
- `undefined`

Modules intégrés

Les modules intégrés suivants sont pris en charge.

Modules

- Cryptographie (hachage et HMAC)
- Chaîne de requête

Cryptographie (hachage et HMAC)

Le module cryptographique (`crypto`) fournit des aides standard en matière de hachage et de code d'authentification de message basé sur le hachage (HMAC). Vous pouvez charger le module en utilisant `require('crypto')`. Le module fournit les méthodes suivantes, qui se comportent exactement comme leurs homologues Node.js.

Méthodes de hachage

`crypto.createHash(`*`algorithm`*`)`

Crée et renvoie un objet de hachage que vous pouvez utiliser pour générer des résumés de hachage à l'aide de l'algorithme donné : `md5`, `sha1` ou `sha256`.

`hash.update(`*`data`*`)`

Met à jour le contenu de hachage avec les `data` données

`hash.digest([encoding])`

Calcule le résumé de toutes les données transmises à l'aide de `hash.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Méthodes HMAC

`crypto.createHmac(algorithm, secret key)`

Crée et renvoie un objet HMAC qui utilise le `algorithm` et la `secret key` donnés. L'algorithme peut être `md5`, `sha1` ou `sha256`.

`hmac.update(data)`

Met à jour le contenu HMAC avec les `data` données.

`hmac.digest([encoding])`

Calcule le résumé de toutes les données transmises à l'aide de `hmac.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Chaîne de requête

> **Note**
>
> L'objet d'événement CloudFront Functions analyse automatiquement les chaînes de requête d'URL pour vous. Cela signifie que, dans la plupart des cas, vous n'avez pas besoin d'utiliser ce module.

Le module de chaînes de requêtes (`querystring`) fournit des méthodes d'analyse et de formatage des chaînes de requêtes URL. Vous pouvez charger le module en utilisant `require('querystring')`. Le module fournit les méthodes suivantes :

`querystring.escape(string)`

Encode par URL la `string` donnée, en renvoyant une chaîne de requêtes échappée. La méthode est utilisée par `querystring.stringify()` et ne doit pas être utilisée directement.

`querystring.parse(string[, separator[, equal[, options]]])`

Analyse une chaîne de requêtes (`string`) et renvoie un objet.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de &.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de =.

Le paramètre `options` est un objet avec les clés suivantes :

`decodeURIComponent` *`function`*

Fonction pour décoder les caractères encodés en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.unescape()`.

`maxKeys` *`number`*

Nombre maximal de clés à analyser. Par défaut, il s'agit de `1000`. Utilisez une valeur de `0` pour supprimer les limitations pour le comptage des clés.

Par défaut, les caractères encodés en pourcentage dans la chaîne de requêtes sont supposés utiliser l'encodage UTF-8. Les séquences UTF-8 non valides sont remplacées par le caractère de remplacement `U+FFFD`.

Par exemple, pour la chaîne de requêtes suivante :

```
'name=value&abc=xyz&abc=123'
```

La valeur renvoyée de `querystring.parse()` est :

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` est un alias pour `querystring.parse()`.

`querystring.stringify(`*`object`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Sérialise un `object` et renvoie une chaîne de requêtes.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de &.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de =.

Le paramètre `options` est un objet avec les clés suivantes :

`encodeURIComponent` *`function`*

Fonction à utiliser pour convertir des caractères non sûrs pour une URL en encodage en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.escape()`.

Par défaut, les caractères qui nécessitent un encodage en pourcentage dans la chaîne de requêtes sont encodés en UTF-8. Pour utiliser un encodage différent, spécifiez l'option `encodeURIComponent`.

Par exemple, pour le code suivant :

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

La valeur renvoyée est :

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` est un alias pour `querystring.stringify()`.

`querystring.unescape(`*`string`*`)`

Décode les caractères encodés en pourcentage URL dans la `string` donnée, en renvoyant une chaîne de requêtes non échappée. Cette méthode est utilisée par `querystring.parse()` et ne doit pas être utilisée directement.

Fonctions limitées

Les fonctionnalités JavaScript linguistiques suivantes ne sont pas prises en charge ou sont restreintes pour des raisons de sécurité.

Évaluation dynamique du code

L'évaluation dynamique du code n'est pas prise en charge. Les deux constructeurs `eval()` et `Function` renvoient une erreur en cas de tentative. Par exemple, `const sum = new Function('a', 'b', 'return a + b')` renvoie une erreur.

Temporisateurs

Les fonctions `setTimeout()`, `setImmediate()` et `clearTimeout()` ne sont pas prises en charge. Il n'y a aucune disposition relative au report ou au produit dans une exécution de fonction. Votre fonction doit s'exécuter de manière synchrone jusqu'à la fin.

Horodatages

Pour des raisons de sécurité, il n'y a pas d'accès aux temporisateurs haute résolution. Toutes les méthodes `Date` pour interroger l'heure actuelle retournent toujours la même valeur pendant la durée de vie d'une même exécution de la fonction. L'horodatage renvoyé est l'heure à laquelle la fonction a commencé à s'exécuter. Par conséquent, vous ne pouvez pas mesurer le temps écoulé dans votre fonction.

Accès au système de fichiers

Il n'y a pas d'accès au système de fichiers. Par exemple, il n'y a pas de module `fs` pour l'accès au système de fichiers comme dans Node.js.

Accès au traitement

Il n'y a aucun accès au traitement. Par exemple, il n'existe pas d'objet global `process` pour accéder aux informations de traitement, comme c'est le cas dans Node.js.

Variables d'environnement

Il n'y a aucun accès aux variables d'environnement.

Vous pouvez plutôt créer une banque CloudFront KeyValueStore de données centralisée de paires clé-valeur pour vos fonctions. CloudFront CloudFront KeyValueStore permet des mises à jour dynamiques de vos données de configuration sans qu'il soit nécessaire de déployer des modifications de code. Vous devez utiliser JavaScript Runtime 2.0 pour utiliser CloudFront KeyValueStore. Pour de plus amples informations, veuillez consulter Amazon CloudFront KeyValueStore.

Accès réseau

Les appels réseau ne sont pas pris en charge. Par exemple, XHR, HTTP(S) et socket ne sont pas pris en charge.

JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions

L'environnement JavaScript d'exécution CloudFront Functions est compatible avec ECMAScript (ES) version 5.1 et prend également en charge certaines fonctionnalités des versions ES 6 à 12. Il fournit

également des méthodes non standard qui ne font pas partie des spécifications ES. Les rubriques suivantes répertorient toutes les fonctionnalités de cet environnement d'exécution.

Rubriques

- Fonctions de base
- Objets primitifs
- Objets intégrés
- Types d'erreurs
- Globals
- Modules intégrés
- Fonctions limitées

Fonctions de base

Les fonctions de base suivantes d'ES sont prises en charge.

Types

Tous les types ES 5.1 sont pris en charge, notamment les valeurs booléennes, les nombres, les chaînes, les objets, les tableaux, les fonctions et les expressions régulières.

Opérateurs

Tous les opérateurs ES 5.1 sont pris en charge.

L'opérateur d'exponentiation ES 7 (`**`) est pris en charge.

Instructions

Les instructions ES 5.1 suivantes sont prises en charge :

- `break`
- `catch`
- `continue`
- `do-while`
- `else`
- `finally`
- `for`

- `for-in`
- `if`
- `label`
- `return`
- `switch`
- `throw`
- `try`
- `var`
- `while`

Les instructions ES 6 suivantes sont prises en charge :

- `const`
- `let`

Les instructions ES 8 suivantes sont prises en charge :

- `async`
- `await`

> **Note**
>
> `async`, `awaitconst`, et `let` sont pris en charge dans JavaScript Runtime 2.0. `await` ne peut être utilisé qu'à l'intérieur de fonctions `async`. Les arguments et fermetures `async` ne sont pas pris en charge.

Littéraux

Les littéraux de modèles ES 6 sont pris en charge : chaînes multiligne, interpolation d'expression et modèles d'imbrication.

Fonctions

Toutes les fonctions ES 5.1 sont prises en charge.

Les fonctions de flèche ES 6 ainsi que la syntaxe des paramètres du reste ES 6 sont prises en charge.

Unicode

Le texte source et les littéraux de chaînes peuvent contenir des caractères Unicode. Les séquences d'échappement de points de code Unicode de six caractères (par exemple `\uXXXX`) sont également prises en charge.

Mode strict

Les fonctions opèrent en mode strict par défaut. Vous n'avez donc pas besoin d'ajouter une instruction `use strict` dans votre code de fonction. Elles ne peuvent pas être modifiées.

Objets primitifs

Les objets primitifs suivants d'ES sont pris en charge.

Objet

Les méthodes ES 5.1 suivantes sur les objets sont prises en charge :

- `Object.create()` (sans liste de propriétés)
- `Object.defineProperties()`
- `Object.defineProperty()`
- `Object.freeze()`
- `Object.getOwnPropertyDescriptor()`
- `Object.getOwnPropertyDescriptors()`
- `Object.getOwnPropertyNames()`
- `Object.getPrototypeOf()`
- `Object.isExtensible()`
- `Object.isFrozen()`
- `Object.isSealed()`
- `Object.keys()`
- `Object.preventExtensions()`
- `Object.seal()`

Les méthodes ES 6 suivantes sur les objets sont prises en charge :

- `Object.assign()`

Les méthodes ES 8 suivantes sur les objets sont prises en charge :

- `Object.entries()`
- `Object.values()`

Les méthodes de prototype d'ES 5.1 suivantes sur les objets sont prises en charge :

- `Object.prototype.hasOwnProperty()`
- `Object.prototype.isPrototypeOf()`
- `Object.prototype.propertyIsEnumerable()`
- `Object.prototype.toString()`
- `Object.prototype.valueOf()`

Les méthodes de prototype d'ES 6 suivantes sur les objets sont prises en charge :

- `Object.prototype.is()`
- `Object.prototype.setPrototypeOf()`

String

Les méthodes ES 5.1 suivantes sur les chaînes sont prises en charge :

- `String.fromCharCode()`

Les méthodes ES 6 suivantes sur les chaînes sont prises en charge :

- `String.fromCodePoint()`

Les méthodes de prototype d'ES 5.1 suivantes sur les chaînes sont prises en charge :

- `String.prototype.charAt()`
- `String.prototype.concat()`
- `String.prototype.indexOf()`
- `String.prototype.lastIndexOf()`
- `String.prototype.match()`
- `String.prototype.replace()`
- `String.prototype.search()`
- `String.prototype.slice()`
- `String.prototype.split()`
- `String.prototype.substr()`
- `String.prototype.substring()`

- `String.prototype.toLowerCase()`
- `String.prototype.trim()`
- `String.prototype.toUpperCase()`

Les méthodes de prototype d'ES 6 suivantes sur les chaînes sont prises en charge :

- `String.prototype.codePointAt()`
- `String.prototype.endsWith()`
- `String.prototype.includes()`
- `String.prototype.repeat()`
- `String.prototype.startsWith()`

Les méthodes de prototype d'ES 8 suivantes sur les chaînes sont prises en charge :

- `String.prototype.padStart()`
- `String.prototype.padEnd()`

Les méthodes de prototype d'ES 9 suivantes sur les chaînes sont prises en charge :

- `String.prototype.trimStart()`
- `String.prototype.trimEnd()`

Les méthodes de prototype d'ES 12 suivantes sur les chaînes sont prises en charge :

- `String.prototype.replaceAll()`

> **Note**
>
> `String.prototype.replaceAll()`est nouveau dans JavaScript Runtime 2.0.

Number

TOUS les nombres d'ES 5 sont pris en charge.

Les propriétés d'ES 6 suivantes sur les nombres sont prises en charge :

- `Number.EPSILON`
- `Number.MAX_SAFE_INTEGER`
- `Number.MIN_SAFE_INTEGER`
- `Number.MAX_VALUE`
- `Number.MIN_VALUE`

- `Number.NaN`
- `Number.NEGATIVE_INFINITY`
- `Number.POSITIVE_INFINITY`

Les méthodes ES 6 suivantes sur les nombres sont prises en charge :

- `Number.isFinite()`
- `Number.isInteger()`
- `Number.isNaN()`
- `Number.isSafeInteger()`
- `Number.parseInt()`
- `Number.parseFloat()`

Les méthodes de prototype d'ES 5.1 suivantes sur les nombres sont prises en charge :

- `Number.prototype.toExponential()`
- `Number.prototype.toFixed()`
- `Number.prototype.toPrecision()`

Les séparateurs numériques d'ES 12 sont pris en charge.

> **Note**
>
> Les séparateurs numériques ES 12 sont nouveaux dans JavaScript Runtime 2.0.

Objets intégrés

Les objets intégrés suivants d'ES sont pris en charge.

Mathématiques

Toutes les méthodes mathématiques ES 5.1 sont prises en charge.

> **Note**
>
> Dans l'environnement d'exécution de CloudFront Functions, l'`Math.random()`implémentation utilise `arc4random` OpenBSD prédéfini avec l'horodatage de l'exécution de la fonction.

Les propriétés mathématiques d'ES 6 suivantes sont prises en charge :

- `Math.E`
- `Math.LN10`
- `Math.LN2`
- `Math.LOG10E`
- `Math.LOG2E`
- `Math.PI`
- `Math.SQRT1_2`
- `Math.SQRT2`

Les méthodes mathématiques ES 6 suivantes sont prises en charge :

- `Math.abs()`
- `Math.acos()`
- `Math.acosh()`
- `Math.asin()`
- `Math.asinh()`
- `Math.atan()`
- `Math.atan2()`
- `Math.atanh()`
- `Math.cbrt()`
- `Math.ceil()`
- `Math.clz32()`
- `Math.cos()`
- `Math.cosh()`
- `Math.exp()`
- `Math.expm1()`
- `Math.floor()`
- `Math.fround()`
- `Math.hypot()`
- `Math.imul()`

- `Math.log()`
- `Math.log1p()`
- `Math.log2()`
- `Math.log10()`
- `Math.max()`
- `Math.min()`
- `Math.pow()`
- `Math.random()`
- `Math.round()`
- `Math.sign()`
- `Math.sinh()`
- `Math.sin()`
- `Math.sqrt()`
- `Math.tan()`
- `Math.tanh()`
- `Math.trunc()`

Date

Toutes les fonctions `Date` ES 5.1 sont prises en charge.

> **Note**
>
> Pour des raisons de sécurité, `Date` renvoie toujours la même valeur (l'heure de début de la fonction) pendant la durée de vie d'une même exécution de la fonction. Pour plus d'informations, consultez Fonctions limitées.

Fonction

Les méthodes de prototype d'ES 5.1 suivantes sont prises en charge :

- `Function.prototype.apply()`
- `Function.prototype.bind()`
- `Function.prototype.call()`

Les constructeurs de fonctions ne sont pas pris en charge.

Expressions régulières

Toutes les fonctions d'expression régulière ES 5.1 sont prises en charge. Le langage d'expression régulière est compatible Perl.

Les propriétés d'accesseur de prototype d'ES 5.1 suivantes sont prises en charge :

- `RegExp.prototype.global`
- `RegExp.prototype.ignoreCase`
- `RegExp.protoype.multiline`
- `RegExp.protoype.source`
- `RegExp.prototype.sticky`
- `RegExp.prototype.flags`

> **Note**
>
> `RegExp.prototype.sticky`et `RegExp.prototype.flags` sont nouveaux dans JavaScript Runtime 2.0.

Les méthodes de prototype d'ES 5.1 suivantes sont prises en charge :

- `RegExp.prototype.exec()`
- `RegExp.prototype.test()`
- `RegExp.prototype.toString()`
- `RegExp.prototype[@@replace]()`
- `RegExp.prototype[@@split]()`

> **Note**
>
> `RegExp.prototype[@@split]()`est nouveau dans JavaScript Runtime 2.0.

Les propriétés d'instance d'ES 5.1 suivantes sont prises en charge :

- `lastIndex`

Les groupes de capture nommés ES 9 sont pris en charge.

JSON

Les méthodes d'ES 5.1 suivantes sont prises en charge :

- `JSON.parse()`
- `JSON.stringify()`

Array

Les méthodes ES 5.1 suivantes sur les tableaux sont prises en charge :

- `Array.isArray()`

Les méthodes ES 6 suivantes sur les tableaux sont prises en charge :

- `Array.of()`

Les méthodes de prototype d'ES 5.1 suivantes sont prises en charge :

- `Array.prototype.concat()`
- `Array.prototype.every()`
- `Array.prototype.filter()`
- `Array.prototype.forEach()`
- `Array.prototype.indexOf()`
- `Array.prototype.join()`
- `Array.prototype.lastIndexOf()`
- `Array.prototype.map()`
- `Array.prototype.pop()`
- `Array.prototype.push()`
- `Array.prototype.reduce()`
- `Array.prototype.reduceRight()`
- `Array.prototype.reverse()`
- `Array.prototype.shift()`
- `Array.prototype.slice()`
- `Array.prototype.some()`
- `Array.prototype.sort()`
- `Array.prototype.splice()`

- `Array.prototype.unshift()`

Les méthodes de prototype d'ES 6 suivantes sont prises en charge :

- `Array.prototype.copyWithin()`
- `Array.prototype.fill()`
- `Array.prototype.find()`
- `Array.prototype.findIndex()`

Les méthodes de prototype d'ES 7 suivantes sont prises en charge :

- `Array.prototype.includes()`

Tableaux typés

Les constructeurs de tableaux typés d'ES 6 suivants sont pris en charge :

- `Float32Array`
- `Float64Array`
- `Int8Array`
- `Int16Array`
- `Int32Array`
- `Uint8Array`
- `Uint8ClampedArray`
- `Uint16Array`
- `Uint32Array`

Les méthodes d'ES 6 suivantes sont prises en charge :

- `TypedArray.from()`
- `TypedArray.of()`

> **Note**
>
> `TypedArray.from()`et `TypedArray.of()` sont nouveaux dans JavaScript Runtime 2.0.

Les méthodes de prototype d'ES 6 suivantes sont prises en charge :

- `TypedArray.prototype.copyWithin()`
- `TypedArray.prototype.every()`
- `TypedArray.prototype.fill()`
- `TypedArray.prototype.filter()`
- `TypedArray.prototype.find()`
- `TypedArray.prototype.findIndex()`
- `TypedArray.prototype.forEach()`
- `TypedArray.prototype.includes()`
- `TypedArray.prototype.indexOf()`
- `TypedArray.prototype.join()`
- `TypedArray.prototype.lastIndexOf()`
- `TypedArray.prototype.map()`
- `TypedArray.prototype.reduce()`
- `TypedArray.prototype.reduceRight()`
- `TypedArray.prototype.reverse()`
- `TypedArray.prototype.some()`
- `TypedArray.prototype.set()`
- `TypedArray.prototype.slice()`
- `TypedArray.prototype.sort()`
- `TypedArray.prototype.subarray()`
- `TypedArray.prototype.toString()`

> **Note**
>
> `TypedArray.prototype.every()`,`TypedArray.prototype.fill()`,`TypedArray.proto`
> et `TypedArray.prototype.some()` sont nouveaux dans JavaScript Runtime 2.0.

ArrayBuffer

Les méthodes ES 6 suivantes ArrayBuffer sont prises en charge :

- `isView()`

Les méthodes de prototypage ES 6 suivantes ArrayBuffer sont prises en charge :

- `ArrayBuffer.prototype.slice()`

Promesse

Les méthodes d'ES 6 suivantes sur les promesses sont prises en charge :

- `Promise.all()`
- `Promise.allSettled()`
- `Promise.any()`
- `Promise.reject()`
- `Promise.resolve()`
- `Promise.race()`

> **Note**
>
> `Promise.all()`, `Promise.allSettled()Promise.any()`, et `Promise.race()` sont nouveaux dans JavaScript Runtime 2.0.

Les méthodes de prototype d'ES 6 suivantes sur les promesses sont prises en charge :

- `Promise.prototype.catch()`
- `Promise.prototype.finally()`
- `Promise.prototype.then()`

DataView

Les méthodes de prototype d'ES 6 suivantes sont prises en charge :

- `DataView.prototype.getFloat32()`
- `DataView.prototype.getFloat64()`
- `DataView.prototype.getInt16()`
- `DataView.prototype.getInt32()`
- `DataView.prototype.getInt8()`
- `DataView.prototype.getUint16()`
- `DataView.prototype.getUint32()`
- `DataView.prototype.getUint8()`
- `DataView.prototype.setFloat32()`

- `DataView.prototype.setFloat64()`
- `DataView.prototype.setInt16()`
- `DataView.prototype.setInt32()`
- `DataView.prototype.setInt8()`
- `DataView.prototype.setUint16()`
- `DataView.prototype.setUint32()`
- `DataView.prototype.setUint8()`

> **Note**
>
> Toutes les méthodes de prototypage de Dataview ES 6 sont nouvelles dans JavaScript Runtime 2.0.

Symbol

Les méthodes d'ES 6 suivantes sont prises en charge :

- `Symbol.for()`
- `Symbol.keyfor()`

> **Note**
>
> Toutes les méthodes Symbol ES 6 sont nouvelles dans JavaScript Runtime 2.0.

TextDecoder

Les méthodes de prototype suivantes sont prises en charge :

- `TextDecoder.prototype.decode()`

Les propriétés d'accesseur de prototype suivantes sont prises en charge :

- `TextDecoder.prototype.encoding`
- `TextDecoder.prototype.fatal`
- `TextDecoder.prototype.ignoreBOM`

TextEncoder

Les méthodes de prototype suivantes sont prises en charge :

- `TextEncoder.prototype.encode()`
- `TextEncoder.prototype.encodeInto()`

Console

Il s'agit d'un objet d'aide pour le débogage. Il ne prend en charge que la méthode `log()`, pour enregistrer les messages de journaux.

> **Note**
>
> CloudFront Les fonctions ne prennent pas en charge la syntaxe des virgules, telle que`console.log('a', 'b')`. Utilisez plutôt le format `console.log('a' + ' ' + 'b')`.

Types d’erreurs

Les objets d’erreurs suivants sont pris en charge :

- `Error`
- `EvalError`
- `InternalError`
- `RangeError`
- `ReferenceError`
- `SyntaxError`
- `TypeError`
- `URIError`

Globals

L’objet `globalThis` est pris en charge.

Les fonctions globales ES 5.1 suivantes sont prises en charge :

- `decodeURI()`
- `decodeURIComponent()`
- `encodeURI()`

- `encodeURIComponent()`
- `isFinite()`
- `isNaN()`
- `parseFloat()`
- `parseInt()`

Les fonctions globales d'ES 6 suivantes sont prises en charge :

- `atob()`
- `btoa()`

> **Note**
>
> `atob()`et `btoa()` sont nouveaux dans JavaScript Runtime 2.0.

Les constantes globales suivantes sont prises en charge :

- `NaN`
- `Infinity`
- `undefined`
- `arguments`

Modules intégrés

Les modules intégrés suivants sont pris en charge.

Modules

- Buffer
- Chaîne de requête
- Cryptographie

Buffer

Le module fournit les méthodes suivantes :

- `Buffer.alloc(size[, fill[, encoding]])`

  Allouez un élément `Buffer`.

  - `size` : taille du tampon. Entrez un entier.
  - `fill`: Facultatif. Entrez une chaîne, un élément `Buffer`, un élément Uint8Array ou un entier. La valeur par défaut est `0`.
  - `encoding`: Facultatif. Quand `fill` est une chaîne, entrez l'une des valeurs suivantes : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.allocUnsafe(size)`

  Allouez un élément `Buffer` non initialisé.

  - `size` : entrez un entier.
- `Buffer.byteLength(value[, encoding])`

  Renvoie la longueur d'une valeur, en octets.

  - `value`: chaîne, `Buffer` TypedArray, Dataview ou Arraybuffer.
  - `encoding`: Facultatif. Quand `value` est une chaîne, entrez l'une des valeurs suivantes : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.compare(buffer1, buffer2)`

  Comparez deux éléments `Buffer` pour faciliter le tri des tableaux. Renvoie `0` s'ils sont identiques, `-1` si `buffer1` figure en premier, ou `1` si `buffer2` figure en premier.

  - `buffer1` : entrez un élément `Buffer`.
  - `buffer2` : entrez un autre élément `Buffer`.
- `Buffer.concat(list[, totalLength])`

  Concaténez plusieurs éléments `Buffer`. Renvoie `0` s'il n'y en a aucun. Renvoie jusqu'à `totalLength`.

  - `list` : entrez une liste d'éléments `Buffer`. Notez que cela sera tronqué à `totalLength`.
  - `totalLength`: Facultatif. Entrez un entier non signé. Utilisez la somme des instances `Buffer` dans la liste si le paramètre est vide.
- `Buffer.from(array)`

  Créez un élément `Buffer` à partir d'un tableau.

  - `array` : entrez un tableau d'octets de `0` à `255`.

- `Buffer.from(arrayBuffer, byteOffset[, length]))`

  Créez une vue à partir de `arrayBuffer`, en commençant par le décalage `byteOffset` avec la longueur `length`.

  - `arrayBuffer` : entrez un tableau `Buffer`.
  - `byteOffset` : entrez un entier.
  - `length`: Facultatif. Entrez un entier.
- `Buffer.from(buffer)`

  Créez une copie de l'élément `Buffer`.

  - `buffer` : entrez un élément `Buffer`.
- `Buffer.from(object[, offsetOrEncoding[, length]])`

  Créez un élément `Buffer` à partir d'un objet. Renvoie `Buffer.from(object.valueOf(), offsetOrEncoding, length)` si `valueOf()` n'est pas égal à l'objet.

  - `object` : entrez un objet.
  - `offsetOrEncoding`: Facultatif. Entrez un entier ou une chaîne d'encodage.
  - `length`: Facultatif. Entrez un entier.
- `Buffer.from(string[, encoding])`

  Créez un élément `Buffer` à partir d'une chaîne.

  - `string` : entrez une chaîne.
  - `encoding`: Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.isBuffer(object)`

  Vérifiez si `object` est un tampon. Renvoie `true` ou `false`.

  - `object` : entrez un objet.
- `Buffer.isEncoding(encoding)`

  Vérifiez si `encoding` est pris en charge. Renvoie `true` ou `false`.

  - `encoding`: Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.

Le module fournit les méthodes de prototype de tampon suivantes :

- `Buffer.prototype.compare(target[, targetStart[, targetEnd[, sourceStart[, sourceEnd]]]])`

  Comparez `Buffer` avec la cible. Renvoie `0` s'ils sont identiques, `1` si `buffer` figure en premier, ou `-1` si `target` figure en premier.

  - `target` : entrez un élément `Buffer`.
  - `targetStart`: Facultatif. Entrez un entier. La valeur par défaut est 0.
  - `targetEnd`: Facultatif. Entrez un entier. La valeur par défaut est la longueur `target`.
  - `sourceStart`: Facultatif. Entrez un entier. La valeur par défaut est 0.
  - `sourceEnd`: Facultatif. Entrez un entier. La valeur par défaut est la longueur de `Buffer`.
- `Buffer.prototype.copy(target[, targetStart[, sourceStart[, sourceEnd]]])`

  Copiez le tampon dans `target`.

  - `target` : entrez un élément `Buffer` ou `Uint8Array`.
  - `targetStart`: Facultatif. Entrez un entier. La valeur par défaut est 0.
  - `sourceStart`: Facultatif. Entrez un entier. La valeur par défaut est 0.
  - `sourceEnd`: Facultatif. Entrez un entier. La valeur par défaut est la longueur de `Buffer`.
- `Buffer.prototype.equals(otherBuffer)`

  Comparez `Buffer` à `otherBuffer`. Renvoie `true` ou `false`.

  - `otherBuffer` : entrez une chaîne.
- `Buffer.prototype.fill(value[, offset[, end][, encoding])`

  Remplissez `Buffer` avec `value`.

  - `value` : entrez une chaîne, `Buffer` ou un entier.
  - `offset`: Facultatif. Entrez un entier.
  - `end`: Facultatif. Entrez un entier.
  - `encoding`: Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.includes(value[, byteOffset][, encoding])`

  Recherchez `value` dans `Buffer`. Renvoie `true` ou `false`.

  - `value` : entrez une chaîne, un élément `Buffer`, `Uint8Array` ou un entier.
  - `byteOffset`: Facultatif. Entrez un entier.

  - `encoding`: Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.indexOf(value[, byteOffset][, encoding])`

  Recherchez le premier élément `value` dans `Buffer`. Retourne `index` s'il est trouvé ou `-1` dans le cas contraire.
  - `value` : entrez une chaîne, `Buffer`, Unit8Array ou un entier compris entre 0 et 255.
  - `byteOffset`: Facultatif. Entrez un entier.
  - `encoding`: Facultatif. Entrez l'un des éléments suivants si `value` est une chaîne : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.lastIndexOf(value[, byteOffset][, encoding])`

  Recherchez le dernier élément `value` dans `Buffer`. Retourne `index` s'il est trouvé ou `-1` dans le cas contraire.
  - `value` : entrez une chaîne, `Buffer`, Unit8Array ou un entier compris entre 0 et 255.
  - `byteOffset`: Facultatif. Entrez un entier.
  - `encoding`: Facultatif. Entrez l'un des éléments suivants si `value` est une chaîne : `utf8`, `hex`, `base64`, `base64url`. La valeur par défaut est `utf8`.
- `Buffer.prototype.readInt8(offset)`

  Lisez `Int8` à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.
- `Buffer.prototype.readIntBE(offset, byteLength)`

  Lisez `Int` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.
  - `byteLength`: Facultatif. Entrez un entier compris entre 1 et 6.
- `Buffer.prototype.readInt16BE(offset)`

  Lisez `Int16` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.
- `Buffer.prototype.readInt32BE(offset)`

  Lisez `Int32` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.
  - `offset` : entrez un entier.

- `Buffer.prototype.readIntLE(offset, byteLength)`

  Lisez `Int` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.readInt16LE(offset)`

  Lisez `Int16` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readInt32LE(offset)`

  Lisez `Int32` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUInt8(offset)`

  Lisez `UInt8` à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUIntBE(offset, byteLength)`

  Lisez `UInt` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.readUInt16BE(offset)`

  Lisez `UInt16` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

- • `offset` : entrez un entier.
- `Buffer.prototype.readUInt32BE(offset)`

  Lisez `UInt32` dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUIntLE(offset, byteLength)`

  Lisez `UInt` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.readUInt16LE(offset)`

  Lisez `UInt16` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readUInt32LE(offset)`

  Lisez `UInt32` dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset` : entrez un entier.
- `Buffer.prototype.readDoubleBE([offset])`

  Lisez une valeur double 64 bits dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset`: Facultatif. Entrez un entier.
- `Buffer.prototype.readDoubleLE([offset])`

  Lisez une valeur double 64 bits dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset`: Facultatif. Entrez un entier.
- `Buffer.prototype.readFloatBE([offset])`

  Lisez une valeur float 32 bits dans l'ordre gros-boutiste à la position `offset` à partir de `Buffer`.

  - `offset`: Facultatif. Entrez un entier.
- `Buffer.prototype.readFloatLE([offset])`

  Lisez une valeur float 32 bits dans l'ordre petit-boutiste à la position `offset` à partir de `Buffer`.

  - `offset`: Facultatif. Entrez un entier.
- `Buffer.prototype.subarray([start[, end]])`

  Renvoie une copie de l'élément `Buffer` décalée et recadrée avec de nouveaux éléments `start` et `end`.

  - `start`: Facultatif. Entrez un entier. La valeur par défaut est 0.
  - `end`: Facultatif. Entrez un entier. La valeur par défaut est la longueur du tampon.
- `Buffer.prototype.swap16()`

  Échangez l'ordre des octets du tableau `Buffer` en le traitant comme un tableau de nombres de 16 bits. La longueur de `Buffer` doit être divisible par 2, sans quoi vous recevrez une erreur.
- `Buffer.prototype.swap32()`

Échangez l'ordre des octets du tableau `Buffer` en le traitant comme un tableau de nombres de 32 bits. La longueur de `Buffer` doit être divisible par 4, sans quoi vous recevrez une erreur.

- `Buffer.prototype.swap64()`

  Échangez l'ordre des octets du tableau `Buffer` en le traitant comme un tableau de nombres de 64 bits. La longueur de `Buffer` doit être divisible par 8, sans quoi vous recevrez une erreur.

- `Buffer.prototype.toJSON()`

  Renvoie l'élément `Buffer` au format JSON.

- `Buffer.prototype.toString([encoding[, start[, end]]])`

  Convertissez l'élément `Buffer`, de `start` à `end`, en chaîne encodée.

  - `encoding`: Facultatif. Entrez l'un des éléments suivants : `utf8`, `hex`, `base64` ou `base64url`. La valeur par défaut est `utf8`.
  - `start`: Facultatif. Entrez un entier. La valeur par défaut est 0.
  - `end`: Facultatif. Entrez un entier. La valeur par défaut est la longueur du tampon.

- `Buffer.prototype.write(string[, offset[, length]][, encoding])`

  Écrivez l'élément `string` encodé dans `Buffer` s'il y a de l'espace, ou un élément `string` tronqué s'il n'y a pas assez d'espace.

  - `string` : entrez une chaîne.
  - `offset`: Facultatif. Entrez un entier. La valeur par défaut est 0.
  - `length`: Facultatif. Entrez un entier. La valeur par défaut est la longueur de la chaîne.
  - `encoding`: Facultatif. Entrez éventuellement l'un des éléments suivants : `utf8`, `hex`, `base64` ou `base64url`. La valeur par défaut est `utf8`.

- `Buffer.prototype.writeInt8(value, offset, byteLength)`

  Écrivez l'élément `value` `Int8` de `byteLength` à la position `offset` dans l'élément `Buffer`.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.writeIntBE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt16BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.
  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt32BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.
  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeIntLE(offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt16LE(offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeInt32LE(offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt8(value, offset, byteLength)`

  Écrivez l'élément `value` `UInt8` de `byteLength` à la position `offset` dans `Buffer`.
  - `value` : entrez un entier.

  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUIntBE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt16BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt32BE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUIntLE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.
- `Buffer.prototype.writeUInt16LE(value, offset, byteLength)`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset` : entrez un entier.
  - `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.writeUInt32LE(value, offset, byteLength)`

Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

- `value` : entrez un entier.
- `offset` : entrez un entier.
- `byteLength` : entrez un entier entre 1 et 6.

- `Buffer.prototype.writeDoubleBE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset`: Facultatif. Entrez un entier. La valeur par défaut est 0.

- `Buffer.prototype.writeDoubleLE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset`: Facultatif. Entrez un entier. La valeur par défaut est 0.

- `Buffer.prototype.writeFloatBE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre gros-boutiste.

  - `value` : entrez un entier.
  - `offset`: Facultatif. Entrez un entier. La valeur par défaut est 0.

- `Buffer.prototype.writeFloatLE(value, [offset])`

  Écrivez `value` à la position `offset` dans `Buffer` en utilisant l'ordre petit-boutiste.

  - `value` : entrez un entier.
  - `offset`: Facultatif. Entrez un entier. La valeur par défaut est 0.

Les méthodes d'instance suivantes sont prises en charge :

- `buffer[index]`

  Obtenez et définissez l'octet (byte) à la position `index` dans l'élément `Buffer`.

  - Obtenez un nombre entre `0` et `255`. Ou définissez un nombre entre `0` et `255`.

Les propriétés d'instance suivantes sont prises en charge :

- `buffer`

  Obtenez l'objet `ArrayBuffer` pour le tampon.

- `byteOffset`

  Obtenez l'élément `byteOffset` de l'objet `Arraybuffer` du tampon.

- `length`

  Obtenez le nombre d'octets du tampon.

> **Note**
>
> Toutes les méthodes du module Buffer sont nouvelles dans JavaScript Runtime 2.0.

Chaîne de requête

> **Note**
>
> L'objet d'événement CloudFront Functions analyse automatiquement les chaînes de requête d'URL pour vous. Cela signifie que, dans la plupart des cas, vous n'avez pas besoin d'utiliser ce module.

Le module de chaînes de requêtes (`querystring`) fournit des méthodes d'analyse et de formatage des chaînes de requêtes URL. Vous pouvez charger le module en utilisant `require('querystring')`. Le module fournit les méthodes suivantes :

`querystring.escape(`*`string`*`)`

Encode par URL la `string` donnée, en renvoyant une chaîne de requêtes échappée. La méthode est utilisée par `querystring.stringify()` et ne doit pas être utilisée directement.

`querystring.parse(`*`string`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Analyse une chaîne de requêtes (`string`) et renvoie un objet.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de &.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de =.

Le paramètre `options` est un objet avec les clés suivantes :

`decodeURIComponent` *`function`*

Fonction pour décoder les caractères encodés en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.unescape()`.

`maxKeys` *`number`*

Nombre maximal de clés à analyser. Par défaut, il s'agit de `1000`. Utilisez une valeur de `0` pour supprimer les limitations pour le comptage des clés.

Par défaut, les caractères encodés en pourcentage dans la chaîne de requêtes sont supposés utiliser l'encodage UTF-8. Les séquences UTF-8 non valides sont remplacées par le caractère de remplacement `U+FFFD`.

Par exemple, pour la chaîne de requêtes suivante :

```
'name=value&abc=xyz&abc=123'
```

La valeur renvoyée de `querystring.parse()` est :

```
{
name: 'value',
abc: ['xyz', '123']
}
```

`querystring.decode()` est un alias pour `querystring.parse()`.

`querystring.stringify(`*`object`*`[, `*`separator`*`[, `*`equal`*`[, `*`options`*`]]])`

Sérialise un `object` et renvoie une chaîne de requêtes.

Le paramètre `separator` est une sous-chaîne permettant de délimiter les paires clé-valeur dans la chaîne de requêtes. Par défaut, il s'agit de &.

Le paramètre `equal` est une sous-chaîne permettant de délimiter les clés et les valeurs dans la chaîne de requêtes. Par défaut, il s'agit de =.

Le paramètre `options` est un objet avec les clés suivantes :

`encodeURIComponent` *`function`*

Fonction à utiliser pour convertir des caractères non sûrs pour une URL en encodage en pourcentage dans la chaîne de requêtes. Par défaut, il s'agit de `querystring.escape()`.

Par défaut, les caractères qui nécessitent un encodage en pourcentage dans la chaîne de requêtes sont encodés en UTF-8. Pour utiliser un encodage différent, spécifiez l'option `encodeURIComponent`.

Par exemple, pour le code suivant :

```
querystring.stringify({ name: 'value', abc: ['xyz', '123'], anotherName: '' });
```

La valeur renvoyée est :

```
'name=value&abc=xyz&abc=123&anotherName='
```

`querystring.encode()` est un alias pour `querystring.stringify()`.

`querystring.unescape(`*`string`*`)`

Décode les caractères encodés en pourcentage URL dans la `string` donnée, en renvoyant une chaîne de requêtes non échappée. Cette méthode est utilisée par `querystring.parse()` et ne doit pas être utilisée directement.

Cryptographie

Le module cryptographique (`crypto`) fournit des aides standard en matière de hachage et de code d'authentification de message basé sur le hachage (HMAC). Vous pouvez charger le module en utilisant `require('crypto')`.

Méthodes de hachage

`crypto.createHash(`*`algorithm`*`)`

Crée et renvoie un objet de hachage que vous pouvez utiliser pour générer des résumés de hachage à l'aide de l'algorithme donné : `md5`, `sha1` ou `sha256`.

`hash.update(`*`data`*`)`

Met à jour le contenu de hachage avec les `data` données

`hash.digest([encoding])`

Calcule le résumé de toutes les données transmises à l'aide de `hash.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Méthodes HMAC

`crypto.createHmac(algorithm, secret key)`

Crée et renvoie un objet HMAC qui utilise le `algorithm` et la `secret key` donnés. L'algorithme peut être `md5`, `sha1` ou `sha256`.

`hmac.update(data)`

Met à jour le contenu HMAC avec les `data` données.

`hmac.digest([encoding])`

Calcule le résumé de toutes les données transmises à l'aide de `hmac.update()`. L'encodage peut être `hex`, `base64` ou `base64url`.

Fonctions limitées

Les fonctionnalités JavaScript linguistiques suivantes ne sont pas prises en charge ou sont restreintes pour des raisons de sécurité.

Évaluation dynamique du code

L'évaluation dynamique du code n'est pas prise en charge. Les deux constructeurs `eval()` et `Function` renvoient une erreur en cas de tentative. Par exemple, `const sum = new Function('a', 'b', 'return a + b')` renvoie une erreur.

Temporisateurs

Les fonctions `setTimeout()`, `setImmediate()` et `clearTimeout()` ne sont pas prises en charge. Il n'y a aucune disposition relative au report ou au produit dans une exécution de fonction. Votre fonction doit s'exécuter de manière synchrone jusqu'à la fin.

Horodatages

Pour des raisons de sécurité, il n'y a pas d'accès aux temporisateurs haute résolution. Toutes les méthodes `Date` pour interroger l'heure actuelle retournent toujours la même valeur pendant la

durée de vie d'une même exécution de la fonction. L'horodatage renvoyé est l'heure à laquelle la fonction a commencé à s'exécuter. Par conséquent, vous ne pouvez pas mesurer le temps écoulé dans votre fonction.

Accès au système de fichiers

Il n'y a pas d'accès au système de fichiers. Par exemple, il n'y a pas de module `fs` pour l'accès au système de fichiers comme dans Node.js.

Accès au traitement

Il n'y a aucun accès au traitement. Par exemple, il n'existe pas d'objet global `process` pour accéder aux informations de traitement, comme c'est le cas dans Node.js.

Variables d'environnement

Il n'y a aucun accès aux variables d'environnement. Vous pouvez plutôt créer une banque CloudFront KeyValueStore de données centralisée de paires clé-valeur pour vos fonctions. CloudFront CloudFront KeyValueStore permet des mises à jour dynamiques de vos données de configuration sans qu'il soit nécessaire de déployer des modifications de code. Pour de plus amples informations, veuillez consulter Amazon CloudFront KeyValueStore.

Accès réseau

Les appels réseau ne sont pas pris en charge. Par exemple, XHR, HTTP(S) et socket ne sont pas pris en charge.

Méthodes d'aide pour les magasins de clés-valeurs

> **Note**
>
> Les appels à la méthode d'assistance au stockage des valeurs clés depuis CloudFront Functions ne déclenchent aucun événement de AWS CloudTrail données. Ces événements ne sont pas enregistrés dans l'historique des CloudTrail événements. Pour plus d'informations, consultez Journalisation des appels CloudFront d'API Amazon à l'aide AWS CloudTrail.

Cette section s'applique si vous utilisez le CloudFront Key Value Store pour inclure des valeurs clés dans la fonction que vous créez. CloudFront Functions possède un module qui fournit trois méthodes d'assistance pour lire les valeurs du magasin de valeurs clés.

Pour utiliser ce module dans le code de fonction, assurez-vous d'avoir associé un magasin de clés-valeurs à la fonction.

Ajoutez ensuite les instructions suivantes dans les premières lignes du code de fonction :

```
import cf from 'cloudfront';
const kvsHandle = cf.kvs();
```

méthode **`get ()`**

Utilisez cette méthode pour renvoyer la valeur associée au nom de clé que vous spécifiez.

Demande

```
get("key", options);
```

- `key` : nom de la clé dont la valeur doit être extraite
- `options` : vous disposez d'une option, `format`. Cela permet de s'assurer que la fonction analyse correctement les données. Valeurs possibles :
  - `string` : (par défaut) encodé en UTF8
  - `json`
  - `bytes` : tampon de données binaires brutes

Exemple de demande

```
const value = await kvsHandle.get("myFunctionKey", { format: "string"});
```

Réponse

La réponse est une `promise` qui aboutit à une valeur au format demandé en grâce aux `options`. Par défaut, la valeur est renvoyée sous forme de chaîne.

Gestion des erreurs

La méthode `get()` renvoie une erreur lorsque la clé que vous avez demandée n'existe pas dans le magasin de clés-valeurs associé. Pour gérer ce cas d'utilisation, vous pouvez ajouter un bloc `try` et `catch` à votre code.

Warning

L'utilisation de combinateurs de promesses (par exemple : `Promise.all`, `Promise.any`) ainsi que de méthodes de chaînage de promesses (par exemple : `then` et `catch`) peut entraîner une utilisation élevée de la mémoire de la fonction. Si votre fonction dépasse le quota de mémoire de fonction maximale, elle ne pourra pas s'exécuter. Pour éviter cette erreur, nous vous recommandons d'utiliser la syntaxe `await` de manière séquentielle ou en boucle pour demander plusieurs valeurs.
Exemple

```
var value1 = await kvs.get('key1');
var value2 = await kvs.get('key2');
```

Actuellement, l'utilisation de combinateurs de promesses pour obtenir plusieurs valeurs n'améliore pas les performances, comme dans l'exemple suivant.

```
var values = await Promise.all([kvs.get('key1'), kvs.get('key2'),]);
```

méthode **`exists ()`**

Utilisez cette méthode pour déterminer si la clé existe ou non dans le magasin de clés-valeurs.

Demande

```
exists("key");
```

Exemple de demande

```
const exist = await kvsHandle.exists("myFunctionkey");
```

Réponse

La réponse est une `promise` qui renvoie une valeur booléenne (`true` ou `false`). Cette valeur indique si la clé existe ou non dans le magasin de clés-valeurs.

méthode **`meta ()`**

Utilisez cette méthode pour renvoyer les métadonnées concernant le magasin de clés-valeurs.

Demande

```
meta();
```

Exemple de demande

```
const meta = await kvsHandle.meta();
```

Réponse

La réponse est un élément `promise` qui se résout à un objet doté des propriétés suivantes :

- `creationDateTime` : date et heure de création du magasin de clés-valeurs, au format ISO 8601.
- `lastUpdatedDateTime` : date et heure de la dernière synchronisation du magasin de clés-valeurs depuis la source, au format ISO 8601. La valeur n'inclut pas la durée de propagation jusqu'à la périphérie.
- `keyCount` : nombre total de clés dans le magasin de clés-valeurs après la dernière synchronisation depuis la source.

Exemple de réponse

```
{keyCount:3,creationDateTime:2023-11-30T23:07:55.765Z,lastUpdatedDateTime:2023-12-15T03:57:52.4
```

Méthodes d'assistance pour la modification de l'origine

Cette section s'applique si vous mettez à jour ou modifiez dynamiquement l'origine utilisée dans la demande dans votre code CloudFront Functions. Vous pouvez mettre à jour l'origine uniquement à la CloudFront demande du spectateur. CloudFront Functions possède un module qui fournit des méthodes d'assistance pour mettre à jour ou modifier dynamiquement l'origine.

Pour utiliser ce module, créez une CloudFront fonction à l'aide de JavaScript Runtime 2.0 et incluez l'instruction suivante dans la première ligne du code de fonction :

```
import cf from 'cloudfront';
```

Pour plus d'informations, consultez JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions.

> **Note**
>
> Les pages de l'API de test et de la console de test ne vérifient pas si une modification de l'origine s'est produite. Cependant, les tests garantissent que le code de fonction s'exécute sans erreur.

Choisissez entre CloudFront Functions et Lambda @Edge

Vous pouvez mettre à jour vos origines en utilisant CloudFront Functions ou Lambda @Edge.

Lorsque vous utilisez CloudFront Functions pour mettre à jour les origines, vous utilisez le déclencheur d'événement de demande du visualiseur, ce qui signifie que cette logique s'exécutera à chaque demande lorsque cette fonction est utilisée. Lorsque vous utilisez Lambda@Edge, les fonctionnalités de mise à jour de l'origine se trouvent sur le déclencheur d'événement demande à l'origine, ce qui signifie que cette logique ne s'exécute qu'en cas d'échec du cache.

Votre choix dépend largement de votre charge de travail et de toute utilisation existante de CloudFront Functions et Lambda @Edge dans vos distributions. Les considérations suivantes peuvent vous aider à décider d'utiliser CloudFront Functions ou Lambda @Edge pour mettre à jour vos origines.

CloudFront Les fonctions sont particulièrement utiles dans les situations suivantes :

- Lorsque vos demandes sont dynamiques (c'est-à-dire qu'elles ne peuvent pas être mises en cache) et qu'elles vont toujours à l'origine. CloudFront Les fonctions offrent de meilleures performances et un coût global inférieur.
- Lorsque vous disposez déjà d'une CloudFront fonction de demande d'affichage qui s'exécute sur chaque demande, vous pouvez ajouter la logique de mise à jour de l'origine à la fonction existante.

Pour utiliser CloudFront Functions pour mettre à jour les origines, consultez les méthodes d'assistance décrites dans les rubriques suivantes.

Lambda@Edge est particulièrement utile dans les cas suivants :

- Lorsque le contenu peut être facilement mis en cache, Lambda @Edge peut être plus rentable car il s'exécute uniquement en cas d'erreur de cache, CloudFront tandis que Functions s'exécute sur chaque requête.

- Lorsque vous disposez déjà d'une fonction Lambda@Edge de type demande à l'origine, vous pouvez y ajouter la logique de mise à jour de l'origine.
- Lorsque votre logique de mise à jour d'origine nécessite de récupérer des données à partir de sources de données tierces, telles qu'Amazon DynamoDB ou Amazon S3.

Pour plus d'informations sur Lambda@Edge, consultez Personnalisation en périphérie avec Lambda@Edge.

méthode update RequestOrigin ()

Utilisez la méthode `updateRequestOrigin()` pour mettre à jour les paramètres d'origine d'une demande. Vous pouvez utiliser cette méthode pour mettre à jour les propriétés d'origine existantes pour les origines déjà définies dans votre distribution, ou pour définir une nouvelle origine pour la demande. Pour ce faire, spécifiez les propriétés que vous souhaitez modifier.

> **Important**
>
> Tous les paramètres que vous ne spécifiez pas dans `updateRequestOrigin()` hériteront des paramètres définis dans la configuration de l'origine existante.

L'origine définie par la `updateRequestOrigin()` méthode peut être n'importe quel point de terminaison HTTP et il n'est pas nécessaire qu'il s'agisse d'une origine existante au sein de votre CloudFront distribution.

> **Remarques**
>
> - Si vous mettez à jour une origine qui fait partie d'un groupe d'origines, seule l'origine principale du groupe d'origines est mise à jour. L'origine secondaire reste inchangée. Tout code de réponse provenant de l'origine modifiée qui correspond aux critères de basculement déclenchera un basculement vers l'origine secondaire.
> - Si vous modifiez le type d'origine et que l'OAC est activé, veillez à ce que le type d'origine dans `originAccessControlConfig` corresponde au nouveau type d'origine.
> - Vous ne pouvez pas utiliser la méthode `updateRequestOrigin()` pour mettre à jour les origines VPC. La demande échouera.

Demande

```
updateRequestOrigin({origin properties})
```

Les `origin properties` peuvent contenir les éléments suivants :

domainName (facultatif)

Nom de domaine de l’origine. Si cette valeur n’est pas fournie, le nom de domaine de l’origine associée est utilisé à la place.

Pour les origines personnalisées

Spécifiez un nom de domaine DNS, tel que `www.example.com`. Le nom de domaine ne peut pas inclure de deux-points (`:`) et ne peut pas être une adresse IP. Le nom du domaine peut contenir jusqu’à 253 caractères.

Pour les origines S3

Spécifiez le nom de domaine DNS du compartiment Amazon S3, tel que `amzn-s3-demo-bucket.s3.eu-west-1.amazonaws.com`. Il peut comporter jusqu’à 128 caractères, qui doivent tous être en minuscules.

HostHeader (facultatif, pour les origines personnalisées autres que S3)

L'en-tête de l'hôte à utiliser lorsque vous envoyez la demande à l'origine. Si ce n'est pas le cas, la valeur du paramètre DomainName est utilisée. Si aucun en-tête d'hôte ou paramètre de nom de domaine n'est fourni, le nom de domaine de l'origine attribuée est utilisé ou l'en-tête de l'hôte de la demande entrante si la politique de transfert vers l'origine (FTO) inclut l'hôte. L'en-tête de l'hôte ne peut pas inclure de deux-points (`:`) et ne peut pas être une adresse IP. L'en-tête de l'hôte peut comporter jusqu'à 253 caractères.

originPath (facultatif)

Chemin de répertoire à l’origine où la demande doit localiser le contenu. Ce chemin doit commencer par une barre oblique (/) mais ne doit pas se terminer par une barre oblique. Par exemple, il ne doit pas se terminer par `example-path/`. Si cette valeur n’est pas fournie, le chemin d’origine de l’origine associée est utilisé.

Pour les origines personnalisées

Le chemin d’accès doit être codé en URL et ne pas dépasser 255 caractères.

customHeaders (facultatif)

Vous pouvez inclure des en-têtes personnalisés dans la requête en spécifiant un nom et une valeur d'en-tête pour chacun d'eux. Le format est différent de celui des en-têtes de demande et de réponse dans la structure de l'événement. Utilisez la syntaxe de paire clé-valeur suivante :

```
{"key1": "value1", "key2": "value2", ...}
```

Vous ne pouvez pas ajouter d'en-têtes non autorisés, et un en-tête portant le même nom ne peut pas déjà être présent dans la demande entrante `headers`. Le nom de l'en-tête doit être en minuscules dans le code de votre fonction. Lorsque CloudFront Functions reconvertit l'objet d'événement en requête HTTP, la première lettre de chaque mot des noms d'en-tête est mise en majuscule et les mots sont séparés par un trait d'union.

Par exemple, si le code de votre fonction ajoute un en-tête nommé`example-header-name`, le CloudFront convertit en en-tête `Example-Header-Name` dans la requête HTTP. Pour plus d'informations, consultez En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine et Restrictions sur les fonctions périphériques.

Si cette valeur n'est pas fournie, les en-têtes personnalisés de l'origine associée sont utilisés.

connectionAttempts (facultatif)

Nombre de CloudFront tentatives de connexion à l'origine. La valeur minimale est 1 et la valeur maximale est 3. Si cette valeur n'est pas fournie, les tentatives de connexion provenant de l'origine attribuée sont utilisées.

originShield (facultatif)

Cela active ou met à jour CloudFront Origin Shield. L'utilisation d'Origin Shield permet de réduire la charge sur votre origine. Pour plus d'informations, consultez Utiliser Amazon CloudFront Origin Shield. Si cette valeur n'est pas fournie, les paramètres Origin Shield de l'origine attribuée sont utilisés.

enabled (obligatoire)

Expression booléenne permettant d'activer ou de désactiver Origin Shield. Accepte la valeur `true` ou `false`.

region (obligatoire lorsqu'elle est activée)

Le Région AWS pour Origin Shield. Spécifiez l' Région AWS dont la latence est la plus faible par rapport à votre origine. Utilisez le code de région et non le nom de la région. Par exemple, utilisez `us-east-2` pour spécifier la région USA Est (Ohio).

Lorsque vous activez CloudFront Origin Shield, vous devez Région AWS le spécifier. Pour obtenir la liste des Régions AWS disponibles et choisir la région la plus appropriée pour votre origine, consultez Cliquez sur l'onglet AWS Région pour Origin Shield.

origine AccessControlConfig (facultatif)

L'identifiant unique d'un contrôle d'accès d'origine (OAC) pour cette origine. Ceci n'est utilisé que lorsque l'origine prend en charge un CloudFront OAC, tel qu'Amazon S3, les URL de fonctions Lambda, les fonctions Web MediaStore Lambda et V2. MediaPackage Si cette valeur n'est pas fournie, les paramètres OAC de l'origine attribuée sont utilisés.

L'identité d'accès d'origine (OAI) héritée n'est pas prise en charge. Pour plus d'informations, consultez Restreindre l'accès à un AWS origine.

enabled (obligatoire)

Expression booléenne permettant d'activer ou de désactiver l'OAC. Accepte la valeur `true` ou `false`.

signingBehavior (obligatoire si activé)

Spécifie les demandes CloudFront signées (ajoute des informations d'authentification à). Spécifiez `always` pour le cas d'utilisation le plus courant. Pour plus d'informations, consultez Paramètres avancés pour le contrôle d'accès à l'origine.

Ce champ peut avoir l'une des valeurs suivantes :

- `always`— CloudFront signe toutes les demandes d'origine, en remplaçant l'`Authorization`en-tête de la demande du lecteur s'il en existe une.
- `never`— CloudFront ne signe aucune demande d'origine. Cette valeur désactive le contrôle d'accès d'origine pour l'origine.
- `no-override`— Si la demande du lecteur ne contient pas l'`Authorization`en-tête, CloudFront signe la demande d'origine. Si la demande du visualiseur contient l'`Authorization`en-tête, CloudFront elle ne signe pas la demande d'origine et transmet à la place l'`Authorization`en-tête de la demande du visualiseur.

> **Warning**
>
> Pour transmettre l'en-tête `Authorization` de la demande de l'utilisateur, vous devez l'ajouter à une politique de demande d'origine pour tous les comportements de cache qui utilisent les origines associées à ce contrôle d'accès d'origine. Pour plus d'informations, consultez Contrôle des demandes d'origine à l'aide d'une stratégie.

- `always-amz-auth`— CloudFront signe toutes les demandes d'origine, mais ne remplace pas l'`Authorization`en-tête de la demande du lecteur. CloudFront ajoute sa signature dans un CloudFront en-tête dédié et transmet l'`Authorization`en-tête du spectateur à l'origine sans modification. Cette valeur est requise pour les origines des fonctions Web Lambda et n'est prise en charge pour aucun autre type d'origine. Pour plus d'informations, consultez Comportement de signature.

signingProtocol (obligatoire si activé)

Protocole de signature de l'OAC, qui détermine la manière dont les demandes sont CloudFront signées (authentifiées). Spécifiez `sigv4` pour la plupart des origines. Spécifiez `sigv4a` une origine de point d' Multi-Region accès Amazon S3 ou une origine de fonction Web Lambda globale.

originType (obligatoire si activé)

Le type d'origine de cet OAC. Les valeurs valides sont les suivantes : `s3`, `mediapackagev2`, `mediastore` et `lambda`.

timeouts (facultatif)

Les délais d'expiration que vous pouvez spécifier CloudFront doivent tenter d'attendre que les origines répondent ou envoient des données. Si cette valeur n'est pas fournie, les paramètres de délai d'attente de l'origine attribuée sont utilisés.

> **Note**
>
> Sauf indication contraire, ces délais prennent en charge les origines personnalisées et Amazon S3.

readTimeout (facultatif)

`readTimeout` s’applique aux deux valeurs suivantes :

- Durée (en secondes) d' CloudFront attente d'une réponse après avoir transmis une demande à l'origine.
- Durée (en secondes) d' CloudFront attente après réception d'un paquet de réponse de l'origine et avant de recevoir le paquet suivant.

Le délai minimum est de 1 seconde et le délai maximum est de 120 secondes. Pour plus d’informations, consultez Délai de réponse.

réponse CompletionTimeout (facultatif)

Durée (en secondes) pendant laquelle une demande provenant CloudFront de l'origine peut rester ouverte et attendre une réponse. Si la réponse complète n'est pas reçue de l'origine à ce moment-là, CloudFront met fin à la connexion.

La valeur de `responseCompletionTimeout` doit être supérieure ou égale à la valeur de `readTimeout`. Pour plus d’informations, consultez Délai d’exécution de la réponse.

conserver AliveTimeout (facultatif)

Ce délai s’applique uniquement aux origines personnalisées, et non aux origines Amazon S3. (Les configurations d’origine S3 ignoreront ces paramètres.)

`keepAliveTimeout`Spécifie la durée pendant CloudFront laquelle vous devez essayer de maintenir la connexion à l'origine après avoir reçu le dernier paquet de la réponse. Le délai minimum est de 1 seconde et le délai maximum est de 120 secondes. Pour plus d’informations, consultez Keep-alive délai d'expiration (origines personnalisées et VPC uniquement).

connectionTimeout (facultatif)

Le nombre de secondes d' CloudFront attente lorsque vous essayez d'établir une connexion avec l'origine. Le délai minimum est de 1 seconde et le délai maximum est de 10 secondes. Pour plus d’informations, consultez Délai de connexion.

personnalisé OriginConfig (facultatif)

Utilisez `customOriginConfig` pour spécifier les paramètres de connexion des origines qui ne sont pas un compartiment Amazon S3. Il existe une exception : vous pouvez spécifier ces

paramètres si le compartiment S3 est configuré avec un hébergement de site web statique. (Les autres types de configurations de compartiment S3 ignoreront ces paramètres.) Si `customOriginConfig` n'est pas renseigné, les paramètres de l'origine attribuée sont utilisés.

port (obligatoire)

Port HTTP CloudFront utilisé pour se connecter à l'origine. Spécifiez le port HTTP sur lequel l'origine personnalisée écoute.

protocol (obligatoire)

Spécifie le protocole (HTTP ou HTTPS) CloudFront utilisé pour se connecter à l'origine. Les valeurs valides sont les suivantes :

- `http`— utilise CloudFront toujours le protocole HTTP pour se connecter à l'origine
- `https`— utilise CloudFront toujours HTTPS pour se connecter à l'origine

sslProtocols (obligatoire)

Une liste qui indique le SSL/TLS protocole minimal à CloudFront utiliser lors de la connexion à votre point d'origine via HTTPS. Les valeurs valides sont les suivantes : `SSLv3`, `TLSv1`, `TLSv1.1` et `TLSv1.2`. Pour plus d'informations, consultez Minimum de protocole SSL d'origine.

IP AddressType (facultatif)

Spécifie le type d'adresse IP CloudFront utilisé pour se connecter à l'origine. Les valeurs valides sont `ipv4`, `ipv6` et `dualstack`. La modification de `ipAddressType` n'est prise en charge que lorsque la propriété `domainName` est également modifiée.

sni (facultatif, pour les origines personnalisées autres que S3)

L'indication du nom du serveur (SNI) est une extension du protocole TLS (Transport Layer Security) par laquelle un client indique le nom d'hôte auquel il tente de se connecter au début du processus de prise de contact TLS. Cette valeur doit correspondre à un nom courant figurant sur un certificat TLS sur votre serveur d'origine. Dans le cas contraire, votre serveur d'origine risque de générer une erreur.

Si ce n'est pas le cas, la valeur du `hostHeader` paramètre est utilisée. Si l'en-tête de l'hôte n'est pas fourni, la valeur du `domainName` paramètre est utilisée.

Si aucun en-tête d'hôte ou paramètre de nom de domaine n'est fourni, le nom de domaine de l'origine attribuée est utilisé ou l'en-tête de l'hôte de la demande entrante si la politique de transfert

vers l'origine (FTO) inclut l'hôte. Le SNI ne peut pas inclure de deux-points (`:`) et ne peut pas être une adresse IP. Le SNI peut comporter jusqu'à 253 caractères.

autorisé CertificateNames (facultatif, pour les origines personnalisées autres que S3)

Vous pouvez inclure une liste de noms de certificats valides à utiliser pour valider le domaine correspondant CloudFront au certificat TLS de votre serveur d'origine lors de la prise de contact TLS avec votre serveur d'origine. Ce champ attend un tableau de noms de domaine valides et peut inclure des domaines génériques, tels que`*.example.com`.

Vous pouvez spécifier jusqu'à 20 noms de certificats autorisés. Chaque nom de certificat peut comporter jusqu'à 64 caractères.

Example– mise à jour de l'origine de la demande Amazon S3

L'exemple suivant modifie l'origine de la demande de l'utilisateur pour la remplacer par un compartiment S3, active l'OAC et réinitialise les en-têtes personnalisés envoyés à l'origine.

```
cf.updateRequestOrigin({
    "domainName" : "amzn-s3-demo-bucket-in-us-east-1.s3.us-east-1.amazonaws.com",
    "originAccessControlConfig": {
        "enabled": true,
        "signingBehavior": "always",
        "signingProtocol": "sigv4",
        "originType": "s3"
    },
    // Empty object resets any header configured on the assigned origin
    "customHeaders": {}
});
```

Example– mise à jour de l'origine de demande Application Load Balancer

L'exemple suivant modifie l'origine de la demande de l'utilisateur pour la remplacer par une origine Application Load Balancer et définit un en-tête personnalisé ainsi que des délais d'attente.

```
cf.updateRequestOrigin({
    "domainName" : "example-1234567890.us-east-1.elb.amazonaws.com",
    "timeouts": {
        "readTimeout": 30,
        "connectionTimeout": 5
    },
    "customHeaders": {
```

```
        "x-stage": "production",
        "x-region": "us-east-1"
    }
});
```

Example– mise à jour vers une origine avec Origin Shield activé

Dans l'exemple suivant, Origin Shield est activé sur l'origine de la distribution. Le code de fonction met à jour uniquement le nom de domaine utilisé pour l'origine et omet tous les autres paramètres facultatifs. Dans ce cas, Origin Shield continuera d'être utilisé avec le nom de domaine d'origine modifié, puisque les paramètres Origin Shield n'ont pas été mis à jour.

```
cf.updateRequestOrigin({
    "domainName" : "www.example.com"
});
```

Example— Actualise l'en-tête de l'hôte, le SNI et les noms des certificats autorisés

> **Warning**
>
> Dans la plupart des cas d'utilisation, vous n'aurez pas besoin d'utiliser ce type de modification pour les demandes envoyées à votre origine. Ces paramètres ne doivent pas être utilisés à moins que vous ne compreniez l'impact de la modification de ces valeurs.

L'exemple suivant remplace le nom de domaine, l'en-tête de l'hôte, le SNI et les certificats autorisés sur la demande par l'origine.

```
cf.updateRequestOrigin({
    "domainName": "www.example.com",
    "hostHeader": "test.example.com",
    "sni": "test.example.net",
    "allowedCertificateNames": ["*.example.com", "*.example.net"],
});
```

méthode select RequestOriginById ()

Utilisez `selectRequestOriginById()` pour mettre à jour une origine existante en sélectionnant une autre origine déjà configurée dans votre distribution. Cette méthode utilise les mêmes paramètres que ceux définis par l'origine mise à jour.

Cette méthode accepte uniquement les origines déjà définies dans la même distribution que celle utilisée lors de l'exécution de la fonction. Les origines sont référencées par l'ID d'origine, qui est le nom d'origine que vous avez défini lors de la configuration de l'origine.

Si une origine VPC est configurée dans votre distribution, vous pouvez utiliser cette méthode pour mettre à jour votre origine vers votre origine VPC. Pour plus d'informations, consultez Restriction de l'accès avec les origines de VPC.

Si vous avez une origine avec le protocole TLS mutuel (mTLS) activé dans votre distribution, vous pouvez utiliser cette méthode pour mettre à jour votre origine vers votre origine m TLS-enabled origin. Pour plus d'informations, consultez Utilisation de CloudFront fonctions avec un TLS mutuel d'origine.

Demande

```
cf.selectRequestOriginById(origin_id, {origin_overrides})
```

Dans l'exemple précédent, `origin_id` il s'agit d'une chaîne qui pointe vers le nom d'origine d'une origine dans la distribution qui exécute la fonction. Le `origin_overrides` paramètre peut contenir les éléments suivants :

HostHeader (facultatif, pour les origines personnalisées autres que S3)

L'en-tête de l'hôte à utiliser lorsque vous envoyez la demande à l'origine. Si ce n'est pas le cas, la valeur du `domainName` paramètre est utilisée.

Si aucun en-tête d'hôte ou paramètre de nom de domaine n'est fourni, le nom de domaine de l'origine attribuée est utilisé ou l'en-tête de l'hôte de la demande entrante si la politique de transfert vers l'origine (FTO) inclut l'hôte. L'en-tête de l'hôte ne peut pas inclure de deux-points (`:`) et ne peut pas être une adresse IP. L'en-tête de l'hôte peut comporter jusqu'à 253 caractères.

sni (facultatif, pour les origines personnalisées autres que S3)

L'indication du nom du serveur (SNI) est une extension du protocole TLS (Transport Layer Security) par laquelle un client indique le nom d'hôte auquel il tente de se connecter au début du processus de prise de contact TLS. Cette valeur doit correspondre à un nom courant figurant sur un certificat TLS sur votre serveur d'origine. Dans le cas contraire, votre serveur d'origine risque de générer une erreur.

Si ce n'est pas le cas, la valeur du `hostHeader` paramètre est utilisée. Si l'en-tête de l'hôte n'est pas fourni, la valeur du `domainName` paramètre est utilisée.

Si aucun en-tête d'hôte ou paramètre de nom de domaine n'est fourni, le nom de domaine de l'origine attribuée est utilisé ou l'en-tête de l'hôte de la demande entrante si la politique de transfert vers l'origine (FTO) inclut l'hôte. Le SNI ne peut pas inclure de deux-points (`:`) et ne peut pas être une adresse IP. Le SNI peut comporter jusqu'à 253 caractères.

autorisé CertificateNames (facultatif, pour les origines personnalisées autres que S3)

Vous pouvez inclure une liste de noms de certificats valides à utiliser pour valider le domaine correspondant CloudFront au certificat TLS de votre serveur d'origine lors de la prise de contact TLS avec votre serveur d'origine. Ce champ attend un tableau de noms de domaine valides et peut inclure des domaines génériques, tels que`*.example.com`.

Vous pouvez spécifier jusqu'à 20 noms de certificats autorisés. Chaque nom de certificat peut comporter jusqu'à 64 caractères.

Demande

```
selectRequestOriginById(origin_id)
```

Dans l’exemple précédent, `origin_id` est une chaîne qui fait référence au nom de l’origine dans la distribution où la fonction s’exécute.

Example– sélection de l’origine de demande Amazon S3

L’exemple suivant sélectionne l’origine nommée `amzn-s3-demo-bucket-in-us-east-1` dans la liste des origines associées à la distribution et applique les paramètres de configuration de l’origine `amzn-s3-demo-bucket-in-us-east-1` à la demande.

```
cf.selectRequestOriginById("amzn-s3-demo-bucket-in-us-east-1");
```

Example– sélection de l’origine de demande Application Load Balancer

L’exemple suivant sélectionne une origine Application Load Balancer nommée `myALB-prod` dans la liste des origines associées à la distribution et applique les paramètres de configuration de l’origine `myALB-prod` à la demande.

```
cf.selectRequestOriginById("myALB-prod");
```

Example— Sélectionnez l'origine de la demande Application Load Balancer et remplacez l'en-tête de l'hôte

Comme dans l'exemple précédent, l'exemple suivant sélectionne une origine Application Load Balancer nommée `myALB-prod` dans la liste des origines associées à la distribution, et applique les paramètres de configuration de `myALB-prod` à la demande. Toutefois, cet exemple remplace la valeur de l'en-tête de l'hôte en utilisant`origin_overrides`.

```
cf.overrideRequestOrigin("myALB-prod",{
        "hostHeader" : "test.example.com"
});
```

méthode create RequestOriginGroup ()

Utilisez `createRequestOriginGroup()` pour définir deux origines à utiliser comme groupe d'origines pour le basculement, dans les scénarios nécessitant une haute disponibilité.

Un groupe d'origine comprend deux origines (une origine principale et une origine secondaire), ainsi qu'un critère de basculement que vous spécifiez. Vous créez un groupe d'origine pour prendre en charge le basculement d'origine. CloudFront Lorsque vous créez ou mettez à jour un groupe d'origine à l'aide de cette méthode, vous pouvez spécifier le groupe d'origine au lieu d'une origine unique. CloudFront basculera de l'origine principale vers l'origine secondaire, en utilisant les critères de basculement.

Si une origine VPC est configurée dans votre distribution, vous pouvez utiliser cette méthode pour créer un groupe d'origines à l'aide de votre origine VPC. Pour plus d'informations, consultez Restriction de l'accès avec les origines de VPC.

Si vous avez une origine pour laquelle le protocole TLS mutuel (mTLS) est activé dans votre distribution, vous pouvez utiliser cette méthode pour créer un groupe d'origine incluant votre origine m. TLS-enabled Pour plus d'informations, consultez Utilisation de CloudFront fonctions avec un TLS mutuel d'origine.

Demande

```
createRequestOriginGroup({origin_group_properties})
```

Dans les exemples précédents, `origin_group_properties` peut contenir les éléments suivants :

originIds (obligatoire)

Tableau de `origin_ids`, où chaque `origin_id` est une chaîne qui pointe vers le nom de l'origine dans la distribution exécutant la fonction. Vous devez fournir deux origines dans le tableau. La première origine de la liste est l'origine principale et la seconde sert d'origine secondaire à des fins de basculement.

OriginOverrides (facultatif)

Quelques paramètres avancés peuvent être remplacés à l'aide du `{origin_overrides}` paramètre. Les `origin overrides` peuvent contenir les éléments suivants :

HostHeader (facultatif, pour les origines personnalisées autres que S3)

L'en-tête de l'hôte à utiliser lorsque vous envoyez la demande à l'origine. Si ce n'est pas le cas, la valeur du `domainName` paramètre est utilisée.

Si aucun en-tête d'hôte ou paramètre de nom de domaine n'est fourni, le nom de domaine de l'origine attribuée est utilisé ou l'en-tête de l'hôte de la demande entrante si la politique de transfert vers l'origine (FTO) inclut l'hôte. L'en-tête de l'hôte ne peut pas inclure de deux-points (`:`) et ne peut pas être une adresse IP. L'en-tête de l'hôte peut comporter jusqu'à 253 caractères.

sni (facultatif, pour les origines personnalisées autres que S3)

L'indication du nom du serveur (SNI) est une extension du protocole TLS (Transport Layer Security) par laquelle un client indique le nom d'hôte auquel il tente de se connecter au début du processus de prise de contact TLS. Cette valeur doit correspondre à un nom courant figurant sur un certificat TLS sur votre serveur d'origine, sinon celui-ci risque de générer une erreur.

Si ce n'est pas le cas, la valeur du `hostHeader` paramètre est utilisée. Si l'en-tête de l'hôte n'est pas fourni, la valeur du `domainName` paramètre est utilisée.

Si aucun en-tête d'hôte ou paramètre de nom de domaine n'est fourni, le nom de domaine de l'origine attribuée est utilisé ou l'en-tête de l'hôte de la demande entrante si la politique de transfert vers l'origine (FTO) inclut l'hôte. Le SNI ne peut pas inclure de deux-points (`:`) et ne peut pas être une adresse IP. Le SNI peut comporter jusqu'à 253 caractères.

autorisé CertificateNames (facultatif, pour les origines personnalisées autres que S3)

Vous pouvez inclure une liste de noms de certificats valides à utiliser pour valider le domaine correspondant CloudFront au certificat TLS de votre serveur d'origine lors de la prise de

contact TLS avec votre serveur d'origine. Ce champ attend un tableau de noms de domaine valides et peut inclure des domaines génériques, tels que`*.example.com`.

Vous pouvez spécifier jusqu'à 20 noms de certificats autorisés. Chaque nom de certificat peut comporter jusqu'à 64 caractères.

selectionCriteria (facultatif)

Sélectionnez si vous souhaitez utiliser les critères de basculement d'origine `default` ou appliquer la logique de basculement basée sur le `media-quality-score`. Les valeurs valides sont les suivantes :

- `default` utilise les critères de basculement, en fonction des codes d'état spécifiés dans `failoverCriteria`. Si vous ne définissez pas `selectionCriteria` dans la fonction, `default` sera utilisé.
- `media-quality-score` est utilisé lorsque la fonctionnalité de routage tenant compte de la qualité média est utilisée.

failoverCriteria (obligatoire)

Ensemble de codes d'état qui, lorsqu'ils sont renvoyés par l'origine principale, CloudFront déclenchent le basculement vers l'origine secondaire. Si vous remplacez un groupe d'origines existant, ce tableau remplacera tous les codes d'état de basculement définis dans la configuration d'origine du groupe d'origines.

Lorsque vous utilisez `media-quality-scoreselectionCriteria`, CloudFront tentera d'acheminer les demandes en fonction du niveau de qualité du média. Si l'origine sélectionnée renvoie un code d'erreur défini dans ce tableau, elle CloudFront basculera vers l'autre origine.

Example– création du groupe d'origines de la demande

L'exemple suivant crée un groupe d'origines pour une demande à l'aide des identifiants d'origine. Ces identifiants d'origine proviennent de la configuration du groupe d'origines de la distribution utilisée pour exécuter cette fonction.

Vous pouvez éventuellement utiliser `originOverrides` pour remplacer les configurations du groupe d'origine pour `snihostHeader`, et`allowedCertificateNames`.

```
import cf from 'cloudfront';
```

```
function handler(event) {
    cf.createRequestOriginGroup({
        "originIds": [
            {
                "originId": "origin-1",
                "originOverrides": {
                    "hostHeader": "hostHeader.example.com",
                    "sni": "sni.example.com",
                    "allowedCertificateNames": ["cert1.example.com",
 "cert2.example.com", "cert3.example.com"]
                }
            },
            {
                "originId": "origin-2",
                "originOverrides": {
                    "hostHeader": "hostHeader2.example.com",
                    "sni": "sni2.example.com",
                    "allowedCertificateNames": ["cert4.example.com",
 "cert5.example.com"]
                }
            }
        ],
        "failoverCriteria": {
            "statusCodes": [500]
        }
    });

    event.request.headers['x-hookx'] = { value: 'origin-overrides' };
    return event.request;
}
```

Méthodes d'assistance pour les propriétés de CloudFront SaaS Manager

Utilisez les fonctions d'assistance suivantes pour CloudFront SaaS Manager afin de récupérer les valeurs de vos distributions multi-locataires dans la fonction que vous créez. Pour utiliser les exemples de cette page, vous devez d'abord créer une CloudFront fonction à l'aide de JavaScript Runtime 2.0. Pour plus d’informations, consultez JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions.

Rubriques

- Groupes de connexions
- Locataires de distribution

Groupes de connexions

Le groupe de connexions associé à vos locataires de distribution possède un nom de domaine.

Pour obtenir cette valeur, utilisez le champ `endpoint` du sous-objet `context` de l'objet d'événement.

Demande

```
const value = event.context.endpoint;
```

Réponse

La réponse est une `string` contenant le nom de domaine du groupe de connexion, par exemple : d111111abcdef8.cloudfront.net. Le champ `endpoint` n'apparaît que lorsque votre fonction est invoquée pour les distributions multi-locataires avec un groupe de connexions associé. Pour plus d'informations, consultez Objet Contexte.

Locataires de distribution

CloudFront Functions possède un module qui permet d'accéder à des valeurs spécifiques des locataires de distribution.

Pour utiliser ce module, ajoutez l'instruction suivante à la première ligne de votre code de fonction :

```
import cf from 'cloudfront';
```

Vous pouvez utiliser les exemples suivants uniquement dans la fonction `handler`, soit directement, soit par le biais d'une fonction appelée de manière imbriquée.

Tenant.idchamp **`de distribution`**

Utilisez ce champ pour obtenir la valeur de l'ID de locataire de distribution.

Demande

```
const value = cf.distributionTenant.id;
```

Réponse

La réponse est une `string` contenant l'ID du locataire de distribution, par exemple : `dt_1a2b3c4d5e6f7`.

Gestion des erreurs

Si votre fonction est invoquée pour une distribution standard, le fait de renseigner le champ `distributionTenant.id` renverra une erreur de type `distributionTenant module is not available`. Pour gérer ce cas d'utilisation, vous pouvez ajouter un bloc `try` et `catch` à votre code.

méthode **`distribution Tenant.parameters.get ()`**

Utilisez cette méthode pour renvoyer la valeur des paramètres du locataire de distribution que vous avez spécifiés.

```
distributionTenant.parameters.get("key");
```

`key` : le nom du paramètre du locataire de distribution pour lequel vous souhaitez récupérer la valeur.

Demande

```
const value = distributionTenant.parameters.get("key");
```

Réponse

La réponse est une `string` contenant la valeur du paramètre du locataire de distribution. Par exemple, si le nom de votre clé est `TenantPath`, la valeur de ce paramètre peut être `tenant1`.

Gestion des erreurs

Vous pourriez recevoir les erreurs suivantes :

- Si votre fonction est invoquée pour une distribution standard, la méthode `distributionTenant.parameters.get()` renverra une erreur de type `distributionTenant module is not available`.
- L'erreur `DistributionTenantParameterKeyNotFound` est renvoyée lorsque le paramètre de locataire de distribution que vous avez spécifié n'existe pas.

Pour gérer ces cas d'utilisation, vous pouvez ajouter un bloc `try` et `catch` à votre code.

Utilisation asynchrone and await

CloudFront Fonctions fournies par JavaScript Runtime Functions 2.0 `async` et `await` syntaxe permettant de gérer `Promise` les objets. Les promesses représentent des résultats différés auxquels il est possible d'accéder en utilisant le `await` mot clé dans les fonctions marquées comme`async`. Diverses nouvelles WebCrypto fonctions utilisent Promises.

Pour plus d'informations sur les objets `Promise`, consultez Promise.

> **Note**
>
> Vous devez utiliser JavaScript Runtime 2.0 pour les exemples de code suivants. `await` ne peut être utilisé qu'à l'intérieur de fonctions `async`. Les arguments et fermetures `async` ne sont pas pris en charge.

```
async function answer() {
    return 42;
}

// Note: async, await can be used only inside an async function. async arguments and
 closures are not supported.

async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
    let answer_value = await answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
}
```

L'exemple de JavaScript code suivant montre comment afficher les promesses avec la méthode de la `then` chaîne. Vous pouvez utiliser `catch` pour visualiser les erreurs.

> **Warning**
>
> L'utilisation de combinateurs de promesses (par exemple : `Promise.all`, `Promise.any`) ainsi que de méthodes de chaînage de promesses (par exemple : `then` et `catch`) peut entraîner une utilisation élevée de la mémoire de la fonction. Si votre fonction dépasse le quota de mémoire de fonction maximale, elle ne pourra pas s'exécuter. Pour éviter cette

erreur, nous vous recommandons d'utiliser la syntaxe `await` plutôt que les méthodes `promise`.

```
async function answer() {
    return 42;
}

async function squared_answer() {
   return answer().then(value => value * value)
}
// Note: async, await can be used only inside an async function. async arguments and
 closures are not supported.
async function handler(event) {
    // var answer_value = answer(); // returns Promise, not a 42 value
    let answer_value = await squared_answer(); // resolves Promise, 42
    console.log("Answer"+answer_value);
    event.request.headers['answer'] = { value : ""+answer_value };
    return event.request;
}
```

Support CWT pour les fonctions CloudFront

Cette section fournit des informations sur la prise en charge des jetons Web CBOR (CWT) dans vos CloudFront fonctions, ce qui permet une authentification et une autorisation sécurisées basées sur des jetons sur les sites périphériques. CloudFront Ce support est fourni sous forme de module, accessible dans votre CloudFront fonction.

Pour utiliser ce module, créez une CloudFront fonction à l'aide de l' JavaScript environnement d'exécution 2.0 et incluez l'instruction suivante dans la première ligne du code de la fonction :

```
import cf from 'cloudfront';
```

Les méthodes associées à ce module sont accessibles via (où * est un caractère générique représentant les différentes fonctions présentes dans le module) :

```
cf.cwt.*
```

Pour plus d'informations, consultez JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions.

Actuellement, le module ne prend en charge que la structure MAC0 avec l'algorithme HS256 (HMAC-SHA256) avec une limite de 1 Ko pour la taille maximale du jeton.

Structure des jetons

Cette section couvre la structure des jetons attendue par le module CWT. Le module s'attend à ce que le jeton soit correctement étiqueté et identifiable (par exemple COSE MAC0). De plus, en ce qui concerne la structure du jeton, le module suit les normes définies par le CBOR Object Signing and Encryption (COSE) [RFC 8152].

```
( // CWT Tag (Tag value: 61) --- optional
    ( // COSE MAC0 Structure Tag (Tag value: 17) --- required
        [
            protectedHeaders,
            unprotectedHeaders,
            payload,
            tag,
        ]
    )
)
```

Example: CWT utilisant la structure COSE MAC0

```
61( // CWT tag
    17( // COSE_MAC0 tag
        [
            { // Protected Headers
                1: 4  // algorithm : HMAC-256-64
            },
            { // Unprotected Headers
                4: h'53796d6d6574726963323536' // kid : Symmetric key id
            },
            { // Payload
                1: "https://iss.example.com", // iss
                2: "exampleUser", // sub
                3: "https://aud.example.com", // aud
                4: 1444064944, // exp
                5: 1443944944, // nbf
                6: 1443944944, // iat
            },
            h'093101ef6d789200' // tag
        ]
```

```
    )
)
```

> **Note**
>
> La balise CWT est facultative lors de la génération de jetons. Cependant, la balise de structure COSE est requise.

méthode validateToken ()

La fonction décode et valide un jeton CWT à l'aide de la clé spécifiée. Si la validation est réussie, le jeton CWT décodé est renvoyé. Dans le cas contraire, cela génère une erreur. Veuillez noter que cette fonction n'effectue aucune validation sur l'ensemble de réclamations.

Demande

```
cf.cwt.validateToken(token, handlerContext{key})
```

Parameters

jeton (obligatoire)

Jeton codé pour validation. Il doit s'agir d'un JavaScript Buffer.

HandlerContext (obligatoire)

JavaScript Objet qui stocke le contexte de l'appel ValidateToken. À l'heure actuelle, seule la propriété clé est prise en charge.

clé (obligatoire)

Clé secrète pour le calcul du résumé des messages. Peut être fourni sous forme de chaîne ou de JavaScript tampon.

Réponse

Lorsque la `validateToken()` méthode renvoie un jeton validé avec succès, la réponse de la fonction est a `CWTObject` au format suivant. Une fois décodées, toutes les clés de réclamation sont représentées sous forme de chaînes.

```
CWTObject {
    protectedHeaders,
    unprotectedHeaders,
    payload
}
```

Exemple - Valider le jeton avec un enfant envoyé dans le cadre du jeton

Cet exemple illustre la validation du jeton CWT, où le kid est extrait de l'en-tête. L'enfant est ensuite transmis à CloudFront Functions KeyValueStore pour récupérer la clé secrète utilisée pour valider le jeton.

```
import cf from 'cloudfront'

const CwtClaims = {
   iss: 1,
   aud: 3,
   exp: 4
}

async function handler(event) {
    try {
        let request = event.request;
        let encodedToken = request.headers['x-cwt-token'].value;
        let kid = request.headers['x-cwt-kid'].value;

        // Retrieve the secret key from the kvs
        let secretKey = await cf.kvs().get(kid);

        // Now you can use the secretKey to decode & validate the token.
        let tokenBuffer = Buffer.from(encodedToken, 'base64url');

        let handlerContext = {
           key: secretKey,
        }

        try {
            let cwtObj = cf.cwt.validateToken(tokenBuffer, handlerContext);

            // Check if token is expired
            const currentTime = Math.floor(Date.now() / 1000); // Current time in
 seconds
            if (cwtObj[CwtClaims.exp] && cwtObj[CwtClaims.exp] < currentTime) {
```

```
                return {
                    statusCode: 401,
                    statusDescription: 'Token expired'
                };
            }
        } catch (error) {
            return {
               statusCode: 401,
               statusDescription: 'Invalid token'
            };
         }
    } catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
     }
    return request;
}
```

Méthode generateToken ()

Cette fonction génère un nouveau jeton CWT à l'aide des paramètres de charge utile et de contexte fournis.

Demande

```
cf.cwt.generateToken(generatorContext, payload)
```

Parameters

Contexte du générateur (obligatoire)

Il s'agit d'un JavaScript objet qui est utilisé comme contexte pour générer le jeton et qui contient les paires clé-valeur suivantes :

CWTtag (facultatif)

Cette valeur est une valeur booléenne qui, si elle est spécifiée`true`, `cwtTag` doit être ajoutée.

CoseTag (obligatoire)

Spécifie le type de balise COSE. Actuellement, ne prend en charge que`MAC0`.

clé (obligatoire)

Clé secrète pour calculer le résumé du message. Cette valeur peut être une chaîne ou JavaScript `Buffer`.

charge utile (obligatoire)

Charge utile du jeton pour l'encodage. La charge utile doit être au `CWTObject` format.

Réponse

Renvoie un JavaScript Buffer contenant le jeton codé.

Example: Générez un jeton CWT

```
import cf from 'cloudfront';

const CwtClaims = {
    iss: 1,
    sub: 2,
    exp: 4
};

const CatClaims = {
    catu: 401,
    catnip: 402,
    catm: 403,
    catr: 404
};

const Catu = {
    host: 1,
    path: 2,
    ext: 3
};

const CatuMatchTypes = {
    prefix_match: 1,
    suffix_match: 2,
    exact_match: 3
};

const Catr = {
    renewal_method: 1,
```

```
    next_renewal_time: 2,
    max_uses: 3
};

async function handler(event) {
    try {
        const response = {
            statusCode: 200,
            statusDescription: 'OK',
            headers: {}
        };

        const commonAccessToken = {
            protected: {
                1: "5",
            },
            unprotected: {},
            payload: {
                [CwtClaims.iss]: "cloudfront-documentation",
                [CwtClaims.sub]: "cwt-support-on-cloudfront-functions",
                [CwtClaims.exp]: 1740000000,
                [CatClaims.catu]: {
                    [Catu.host]: {
                        [CatuMatchTypes.suffix_match]: ".cloudfront.net"
                    },
                    [Catu.path]: {
                        [CatuMatchTypes.prefix_match]: "/media/live-stream/cf-4k/"
                    },
                    [Catu.ext]: {
                        [CatuMatchTypes.exact_match]: [
                            ".m3u8",
                            ".ts",
                            ".mpd"
                        ]
                    }
                },
                [CatClaims.catnip]: [
                    "[IP_ADDRESS]",
                    "[IP_ADDRESS]"
                ],
                [CatClaims.catm]: [
                    "GET",
                    "HEAD"
                ],
```

```
                [CatClaims.catr]: {
                    [Catr.renewal_method]: "header_renewal",
                    [Catr.next_renewal_time]: 1750000000,
                    [Catr.max_uses]: 5
                }
            }
        };

        if (!request.headers['x-cwt-kid']) {
            throw new Error('Missing x-cwt-kid header');
        }

        const kid = request.headers['x-cwt-kid'].value;
        const secretKey = await cf.kvs().get(kid);

        if (!secretKey) {
            throw new Error('Secret key not found for provided kid');
        }

        try {
            const genContext = {
                cwtTag: true,
                coseTag: "MAC0",
                key: secretKey
            };

            const tokenBuffer = cf.cwt.generateToken(commonAccessToken, genContext);
            response.headers['x-generated-cwt-token'] = { value:
tokenBuffer.toString('base64url') };

            return response;
        } catch (tokenError) {
            return {
                statusCode: 401,
                statusDescription: 'Could not generate the token'
            };
        }
    } catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
    }
```

```
}
```

Example: actualisez le jeton en fonction d'une certaine logique

```
import cf from 'cloudfront'

const CwtClaims = {
   iss: 1,
   aud: 3,
   exp: 4
}

async function handler(event) {
    try {
        let request = event.request;
        let encodedToken = request.headers['x-cwt-token'].value;
        let kid = request.headers['x-cwt-kid'].value;
        let secretKey = await cf.kvs().get(kid); // Retrieve the secret key from the
 kvs

        // Now you can use the secretKey to decode & validate the token.
        let tokenBuffer = Buffer.from(encodedToken, 'base64url');

        let handlerContext = {
           key: secretKey,
        }

        try {
            let cwtJSON = cf.cwt.validateToken(tokenBuffer, handlerContext);

            // Check if token is expired
            const currentTime = Math.floor(Date.now() / 1000); // Current time in
 seconds
            if (cwtJSON[CwtClaims.exp] && cwtJSON[CwtClaims.exp] < currentTime) {
                // We can regnerate the token and add 8 hours to the expiry time
                cwtJSON[CwtClaims.exp] = Math.floor(Date.now() / 1000) + (8 * 60 * 60);

                let genContext = {
                  coseTag: "MAC0",
                  key: secretKey
                }

                let newTokenBuffer = cf.cwt.generateToken(cwtJSON, genContext);
```

```
                request.headers['x-cwt-regenerated-token'] =
 newTokenBuffer.toString('base64url');
            }
        } catch (error) {
            return {
               statusCode: 401,
               statusDescription: 'Invalid token'
            };
         }
    }
    catch (error) {
        return {
            statusCode: 402,
            statusDescription: 'Token processing failed'
        };
     }
    return request;
}
```

Méthodes d'assistance générales

Cette page fournit des méthodes d'assistance supplémentaires dans CloudFront Functions. Pour utiliser ces méthodes, créez une CloudFront fonction à l'aide de JavaScript Runtime 2.0.

```
import cf from 'cloudfront';
```

Pour de plus amples informations, veuillez consulter JavaScript fonctionnalités d'exécution 2.0 pour CloudFront Functions.

`Métadonnées EdgeLocation`

Cette méthode nécessite l'utilisation du `cloudfront` module.

> **Note**
>
> Vous ne pouvez utiliser cette méthode que pour les fonctions de demande de visualisation. Pour les fonctions de réponse du spectateur, cette méthode est vide.

Utilisez cet JavaScript objet pour obtenir le code d'aéroport de localisation périphérique, la région de cache périphérique régionale attendue ou l'adresse IP CloudFront du serveur utilisée pour traiter

la demande. Ces métadonnées ne sont disponibles que pour le déclencheur de l'événement de demande du spectateur.

```
cf.edgeLocation = {
    name: SEA
    serverIp: 1.2.3.4
    region: us-west-2
}
```

L'`cf.edgeLocation`objet peut contenir les éléments suivants :

name

Code IATA à trois lettres de l'emplacement périphérique qui a traité la demande.

IP du serveur

Adresse IPv4 ou IPv6 du serveur qui a traité la demande.

region

Le cache périphérique CloudFront régional (REC) que la demande est censée utiliser en cas d'échec du cache. Cette valeur n'est pas mise à jour si le REC attendu n'est pas disponible et qu'un REC de sauvegarde est utilisé pour la demande. Cela n'inclut pas l'emplacement d'Origin Shield utilisé, sauf dans les cas où le REC principal et l'Origin Shield se trouvent au même emplacement.

> **Note**
>
> CloudFront Functions n'est pas invoquée une deuxième fois lorsqu'il CloudFront est configuré pour utiliser le basculement d'origine. Pour de plus amples informations, veuillez consulter Optimisez la haute disponibilité grâce au basculement CloudFront d'origine.

méthode raw QueryString ()

Cette méthode ne nécessite pas le `cloudFront` module.

Utilisez la `rawQueryString()` méthode pour récupérer la chaîne de requête non analysée et non modifiée sous forme de chaîne.

Demande

```
function handler(event) {
    var request = event.request;
    const qs = request.rawQueryString();
}
```

Réponse

Renvoie la chaîne de requête complète de la demande entrante sous forme de valeur de chaîne sans le début?.

- S'il n'y a pas de chaîne de requête mais qu'elle ? est présente, les fonctions renvoient une chaîne vide.
- S'il n'y a pas de chaîne de requête et qu'elle ? n'est pas présente, la fonction renvoie`undefined`.

Cas 1 : chaîne de requête complète renvoyée (sans début**?**)

URL de la demande entrante : `https://example.com/page?name=John&age=25&city=Boston`

`rawQueryString()`renvoie : `"name=John&age=25&city=Boston"`

Cas 2 : chaîne vide renvoyée (lorsqu'elle **?** est présente mais sans paramètres)

URL de la demande entrante : `https://example.com/page?`

`rawQueryString()`renvoie : `""`

Cas 3 : **`undefined`** renvoyé (aucune chaîne de requête et non**?**)

URL de la demande entrante : `https://example.com/page`

`rawQueryString()`renvoie : `undefined`

méthode log CustomData ()

Pour utiliser cette méthode, importez le `cloudfront` module.

Utilisez `logCustomData()` cette méthode pour envoyer des données personnalisées depuis votre CloudFront fonction Amazon dans les journaux CloudFront d'accès. Les données sont écrites dans le champ `viewer-request-log-data` ou dans le champ `viewer-response-log-data` journal, selon que la fonction est associée à une demande du spectateur ou à un événement de réponse du spectateur.

La méthode accepte un seul argument de chaîne. Pour enregistrer un objet, `JSON.stringify()` convertissez-le d'abord en chaîne. Par exemple :

```
const resp_obj = JSON.stringify(some_obj);
cf.logCustomData(resp_obj);
```

Chaque champ prend en charge jusqu'à 800 octets de données. CloudFront automatiquement URL-encodes les données avant de les écrire dans le champ du journal. CloudFront tronque ensuite toutes les données supérieures à 800 octets. URL-encoding Si votre fonction appelle `logCustomData()` plusieurs fois au cours d'une même exécution, CloudFront utilise uniquement la dernière valeur.

Ajoutez des champs à la configuration de votre journal

Pour recevoir ces données dans vos journaux CloudFront d'accès, vous devez ajouter les `viewer-response-log-data` champs `viewer-request-log-data` ou à votre configuration de journal en temps réel ou à votre configuration de journalisation standard (v2).

Différence par rapport à console.log ()

La `logCustomData()` méthode ne remplace pas `console.log()` pour CloudFront Functions. Utilisez-le `console.log()` pour envoyer des lignes de journal à Amazon CloudWatch Logs. Permet `cf.logCustomData()` d'écrire des données personnalisées pour CloudFront accéder aux journaux (journaux en temps réel et journalisation standard (v2)). Vous pouvez utiliser les deux méthodes dans la même fonction. Pour plus d'informations, consultez la section Journaux des CloudFront fonctions.

La méthode utilise la syntaxe suivante :

```
cf.logCustomData(String);
```

Example Enregistrer un en-tête dans une fonction de demande de visualisation

```
import cf from 'cloudfront';

function handler(event) {
```

```
    var request = event.request;

    // Check if the debug header exists, if so log it
    if (request.headers['x-debug-header']) {
        // Log the debug header value
        cf.logCustomData("debug header found: " + request.headers['x-debug-
header'].value);
    }

    return request;
}
```

Méthodes auxiliaires pour le protocole TLS mutuel

CloudFront fournit des fonctions d'TLS-specific assistance m dans l'espace de `cf.mtls` noms pour les fonctions de demande du spectateur. Ces fonctions permettent de renommer, reformater ou combiner les en-têtes des certificats clients avant de transmettre la demande à votre point d'origine.

```
import cf from "cloudfront";
```

`cf.mtls.rename ClientCertHeaders`

Renomme les en-têtes des métadonnées des certificats en noms d'en-tête personnalisés.

```
cf.mtls.renameClientCertHeaders({
    "CloudFront-Viewer-Cert-Pem": "X-Client-Cert",
    "CloudFront-Viewer-Cert-Serial-Number": "X-Client-Cert-Serial",
    "CloudFront-Viewer-Cert-Issuer": "X-Client-Cert-Issuer",
});
```

En-têtes de source autorisés :

- `CloudFront-Viewer-Cert-Pem`
- `CloudFront-Viewer-Cert-Serial-Number`
- `CloudFront-Viewer-Cert-Issuer`
- `CloudFront-Viewer-Cert-Subject`
- `CloudFront-Viewer-Cert-Validity`
- `CloudFront-Viewer-Cert-Present`

- `CloudFront-Viewer-Cert-Sha256`
- `Client-Cert`
- `Client-Cert-Chain`

`cf.mtls.rename PemHeaders`

Renomme les en-têtes des certificats PEM et reformate éventuellement le codage du certificat.

```
cf.mtls.renamePemHeaders({
    "Client-Cert": {
        "newHeaderName": "X-Leaf-Cert",
        "pemCertFormatInfo": {
            "certHeader": "-----CUSTOM HEADER-----",
            "certFooter": "-----CUSTOM FOOTER-----",
            "certEndMarker": "",
            "keepNewlinesInCertData": true
        }
    },
    "Client-Cert-Chain": {
        "newHeaderName": "X-Intermediate-Certs",
        "pemCertFormatInfo": {
            "certHeader": "-----CUSTOM HEADER-----",
            "certFooter": "-----CUSTOM FOOTER-----",
            "certEndMarker": "",
            "keepNewlinesInCertData": true
        }
    }
});
```

En-têtes de source autorisés :

- En mode passthrough :`Client-Cert`, `Client-Cert-Chain`
- En required/optional mode : `Cloudfront-Viewer-Cert-PEM`

`pemCertFormatInfo`domaines :

Pour `Cloudfront-Viewer-Cert-PEM` :

- `certHeader` remplace `-----BEGIN CERTIFICATE-----`.
- `certFooter` remplace `-----END CERTIFICATE-----`.

- `certEndMarker`définit une chaîne personnalisée après le CertFooter.
- `keepNewlinesInCertData`(par défaut :`true`) préserve les nouvelles lignes dans les données base64 lorsque c'est vrai.

Pour `Client-Cert` et `Client-Cert-Chain` :

- `certHeader` remplace `:`.
- `certFooter` remplace `:`.
- `certEndMarker`définit une chaîne personnalisée après le CertFooter.
- `keepNewlinesInCertData`(par défaut :`false`) préserve les nouvelles lignes dans les données base64 lorsque c'est vrai.

`cf.mtls.combine PemHeaders`

Combine `Client-Cert` et `Client-Cert-Chain` en un seul en-tête contenant la chaîne de certificats complète.

```
cf.mtls.combinePemHeaders({
    "newHeaderName": "X-Full-Chain",
    "pemCertFormatInfo": {
        "certHeader": "-----BEGIN CERTIFICATE-----",
        "certFooter": "-----END CERTIFICATE-----",
        "certEndMarker": "\n",
        "keepNewlinesInCertData": false
    }
});
```

`certEndMarker`définit le délimiteur entre les certificats.

> **Note**
>
> - Ces fonctions d'assistance peuvent être utilisées dans tous les modes mTLS (obligatoire, optionnel et direct). Cependant, cela `cf.mtls.combinePemHeaders` n'a d'effet qu'en mode relais : dans les modes obligatoire et facultatif, les `Client-Cert-Chain` en-têtes `Client-Cert` et ne sont pas présents, la fonction est donc inopérante.
> - Si `cf.mtls.*` les méthodes et `cf.updateRequestOrigin()` la `customHeaders` cible ont le même nom d'en-tête, CloudFront renvoie une erreur 502.

- En mode Passthrough, CloudFront supprime les entrées `Client-Cert` ou les `Client-Cert-Chain` en-têtes et les ajoute à nouveau à partir du certificat client réel.
- CloudFront ne présente le contenu brut complet du certificat PEM dans aucune fonction de périphérie.

Création de fonctions

La création d'une fonction se déroule en deux temps :

1. Créez le code de fonction sous la forme JavaScript. Vous pouvez utiliser l'exemple par défaut de la CloudFront console ou écrire le vôtre. Pour plus d'informations, consultez les rubriques suivantes :
   - Écriture du code de la fonction
   - the section called "Structure d'évènements"
   - CloudFront Exemples de fonctions pour CloudFront
2. CloudFront Utilisez-le pour créer la fonction et inclure votre code. Le code existe à l'intérieur de la fonction (et non en tant que référence).

Console

Pour créer une fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et choisissez la page Fonctions.
2. Choisissez Créer une fonction.
3. Entrez un nom de fonction unique dans le Compte AWS, choisissez la JavaScript version, puis choisissez Continuer. La page de détails s'affiche pour la nouvelle fonction.

> **Note**
>
> Pour utiliser des paires clé-valeur dans la fonction, vous devez choisir le JavaScript runtime 2.0.
> Si vous rencontrez une erreur `TaggingConflict` (HTTP 409) lors de la création d'une fonction avec des balises, attendez quelques minutes et réessayez, ou créez d'abord la fonction sans balises et ajoutez-les ensuite.

4. Dans la section Code de fonction, sélectionnez l'onglet Création et entrez votre code de fonction. L'exemple de code inclus dans l'onglet Création illustre la syntaxe de base du code de fonction.
5. Cliquez sur Enregistrer les modifications.
6. Si le code de fonction utilise des paires clé-valeur, vous devez associer un magasin de clés-valeurs.

   Vous pouvez associer le magasin de clés-valeurs lors de la création initiale de la fonction. Ou, vous pouvez l'associer ultérieurement, en mettant à jour la fonction.

   Pour associer un magasin de clés-valeurs dès maintenant, procédez comme suit :

   - Accédez à la KeyValueStore section Associer et choisissez Associer existant KeyValueStore.
   - Sélectionnez le magasin de valeurs clés qui contient les paires clé-valeur de la fonction, puis choisissez Associer. KeyValueStore

   CloudFront associe immédiatement le magasin à la fonction. Vous n'avez pas besoin d'enregistrer la fonction.

CLI

Si vous utilisez la CLI, vous commencez généralement par créer le code de fonction dans un fichier, puis vous créez la fonction avec AWS CLI.

Pour créer une fonction

1. Créez le code de fonction dans un fichier et stockez-le dans un répertoire auquel votre ordinateur peut se connecter.
2. Exécutez la commande, comme illustré dans l'exemple. Cet exemple utilise la notation `fileb://` pour transmettre le fichier. Il inclut également des sauts de ligne pour rendre la commande plus lisible.

```
aws cloudfront create-function \
    --name MaxAge \
    --function-config '{"Comment":"Max Age 2 years","Runtime":"cloudfront-
js-2.0","KeyValueStoreAssociations":{"Quantity":1,"Items":
[{"KeyValueStoreARN":"arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"}]}}' \
```

```
    --function-code fileb://function-max-age-v1.js
```

> **Remarques**
>
> - `Runtime`— La version de JavaScript. Pour utiliser des paires clé-valeur dans la fonction, vous devez spécifier la version 2.0.
> - `KeyValueStoreAssociations` : si votre fonction utilise des paires clé-valeur, vous pouvez associer le magasin de clés-valeurs lors de la création initiale de la fonction. Ou vous pouvez l'associer ultérieurement, en utilisant `update-function`. `Quantity` a toujours pour valeur 1, car chaque fonction peut être associée uniquement à un seul magasin de clés-valeurs.

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
ETag: ETVABCEXAMPLE
FunctionSummary:
  FunctionConfig:
    Comment: Max Age 2 years
    Runtime: cloudfront-js-2.0
    KeyValueStoreAssociations= \
      {Quantity=1, \
      Items=[{KeyValueStoreARN='arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111'}]} \
  FunctionMetadata:
    CreatedTime: '2021-04-18T20:38:56.915000+00:00'
    FunctionARN: arn:aws:cloudfront::111122223333:function/MaxAge
    LastModifiedTime: '2023-11-19T20:38:56.915000+00:00'
    Stage: DEVELOPMENT
  Name: MaxAge
  Status: UNPUBLISHED
Location: https://cloudfront.amazonaws.com/2020-05-31/function/
arn:aws:cloudfront:::function/MaxAge
```

La plupart des informations proviennent de la demande. D'autres informations sont ajoutées par CloudFront.

Remarques

- `ETag` : cette valeur change chaque fois que vous modifiez le magasin de clés-valeurs. Vous utilisez cette valeur et le nom de la fonction pour référencer la fonction à l'avenir. Assurez-vous de toujours utiliser l'`ETag` actuel.
- `FunctionARN`— L'ARN de votre CloudFront fonction.
- 111122223333 — Le. Compte AWS
- `Stage` : le stade de la fonction (`LIVE` ou `DEVELOPMENT`).
- `Status` : l'état de la fonction (`PUBLISHED` ou `UNPUBLISHED`).

Une fois que vous avez créé la fonction, elle est ajoutée à la phase `DEVELOPMENT`. Nous vous recommandons de tester votre fonction avant de la publier. Une fois que vous avez publié votre fonction, celle-ci passe à la phase `LIVE`.

TaggingConflict erreur lors de la création de fonctions

CloudFront Les fonctions réutilisent les ARN pour les fonctions portant le même nom. Vous pouvez rencontrer une erreur `TaggingConflict` (HTTP 409) lors de la création d'une fonction avec des balises. Cela peut se produire dans les scénarios suivants :

- Après la suppression d'une fonction — Recréer une fonction avec le même nom et les mêmes balises immédiatement après la suppression.
- Après une tentative de création échouée — Si une demande de création précédente a échoué (par exemple, en raison de paramètres non valides, d'une association KVS non valide ou d'un échec de restauration de CloudFormation pile).

Si vous recevez un `TaggingConflict` message d'erreur, vous pouvez :

- Patientez quelques minutes et recommencez l'opération.
- Utilisez un autre nom de fonction. Cela permet d'éviter complètement le conflit de réutilisation de l'ARN.

- Si votre modèle crée à la fois une fonction KeyValueStore et une fonction qui y fait référence, ajoutez-en une `DependsOn` explication pour vous assurer que le KVS est entièrement provisionné avant la création de la fonction.

Fonctions de test

Avant de déployer la fonction en phase réelle (production), vous pouvez la tester afin de vérifier qu'elle fonctionne comme prévu. Pour tester une fonction, vous devez spécifier un objet d'événement qui représente une requête ou une réponse HTTP que votre CloudFront distribution pourrait recevoir en production.

CloudFront Functions effectue les opérations suivantes :

1. Exécute la fonction, en utilisant l'objet d'événement fourni comme entrée.
2. Renvoie le résultat de la fonction (l'objet d'évènement modifié) ainsi que les journaux de fonction ou les messages d'erreurs et l'utilisation du calcul de la fonction. Pour plus d'informations sur l'utilisation du calcul, consultez the section called “Présentation de l’utilisation du calcul”.

> **Note**
>
> Lorsque vous testez une fonction, elle CloudFront ne valide que par rapport aux erreurs d'exécution de la fonction. CloudFrontne valide pas si la demande sera traitée correctement une fois publiée. Par exemple, si votre fonction supprime un en-tête obligatoire, le test sera validé puisqu'aucune erreur n'est détectée dans le code. Toutefois, si vous publiez la fonction et que vous l'associez à une distribution, elle échouera lorsqu'une demande sera envoyée CloudFront.

Table des matières

- Configuration de l’objet d’événement
- Tester la fonction
- Présentation de l’utilisation du calcul

Configuration de l’objet d’événement

Avant de tester une fonction, vous devez configurer l’objet d’événement avec lequel la tester. Il existe plusieurs options.

Option 1 : configurer un objet d’événement sans l’enregistrer

Vous pouvez configurer un objet d'événement dans l'éditeur visuel de la CloudFront console sans l'enregistrer.

Vous pouvez utiliser cet objet d'événement pour tester la fonction depuis la CloudFront console, même si elle n'est pas enregistrée.

Option 2 : créer un objet d’événement dans l’éditeur visuel

Vous pouvez configurer un objet d'événement dans l'éditeur visuel de la CloudFront console sans l'enregistrer. Vous pouvez créer 10 objets d’événement pour chaque fonction afin de pouvoir, par exemple, tester différentes entrées possibles.

Lorsque vous créez l'objet d'événement de cette manière, vous pouvez l'utiliser pour tester la fonction dans la CloudFront console. Vous ne pouvez pas l'utiliser pour tester la fonction à l'aide d'une AWS API ou d'un SDK.

Option 3 : créer un objet d’événement à l’aide d’un éditeur de texte

Vous pouvez utiliser un éditeur de texte pour créer un objet d’événement au format JSON. Pour en savoir plus sur la structure d’un objet d’événement, consultez Structure d’évènements.

Vous pouvez utiliser cet objet d’événement pour tester la fonction à l’aide de la CLI. Mais vous ne pouvez pas l'utiliser pour tester la fonction dans la CloudFront console.

Pour créer un objet d’évènement (option 1 ou 2)

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.

   Choisissez la fonction que vous souhaitez tester.
2. Sur la page de détails de la fonction, choisissez l’onglet Test.
3. Pour Type d’événement, choisissez l’une des options suivantes :

- Choisissez Demande de l'utilisateur si la fonction modifie une requête HTTP ou génère une réponse basée sur la demande. La section Demande apparaît.
- Choisissez Réponse de l'utilisateur. Les sections Demande et Réponse apparaissent.

4. Complétez les champs que vous souhaitez inclure dans l'événement. Vous pouvez choisir Modifier JSON pour afficher le code JSON brut.
5. (Facultatif) Pour enregistrer l'événement, choisissez Enregistrer et dans le champ Enregistrer l'événement de test, entrez un nom, puis sélectionnez Enregistrer.

   Vous pouvez également choisir Modifier le JSON, copier le JSON brut et l'enregistrer dans votre propre fichier, en dehors de CloudFront.

Pour créer un objet d'évènement (option 3)

Créez l'objet d'événement à l'aide d'un éditeur de texte. Stockez le fichier dans un répertoire auquel votre ordinateur peut se connecter.

Assurez-vous de suivre les consignes suivantes :

- Omettez les champs `distributionDomainName`, `distributionId` et `requestId`.
- Les noms des en-têtes, des cookies et des chaînes de requête doivent être en minuscule.

Une option permettant de créer un objet d'événement de cette manière consiste à créer un échantillon à l'aide de l'éditeur visuel. Vous pouvez être sûr que l'échantillon est correctement formaté. Vous pouvez ensuite copier le code JSON brut, le coller dans un éditeur de texte et enregistrer le fichier.

Pour plus d'informations sur la structure d'un évènement, consultez Structure d'évènements.

Tester la fonction

Vous pouvez tester une fonction dans la CloudFront console ou avec le AWS Command Line Interface (AWS CLI).

Console

Pour tester la fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Choisissez la fonction que vous souhaitez tester.
3. Choisissez l'onglet Test.
4. Assurez-vous que l'événement correct est affiché. Pour remplacer l'événement actuellement affiché, choisissez un autre événement dans le champ Sélectionnez un événement de test.
5. Choisissez Fonction de test. La console affiche la sortie de la fonction, y compris les journaux de la fonction et l'utilisation du calcul.

CLI

Vous pouvez tester une fonction à l'aide de la commande aws cloudfront test-function.

Pour tester la fonction

1. Ouvrez une fenêtre de ligne de commande.
2. Exécutez la commande suivante depuis le même répertoire que celui qui contient le fichier indiqué.

   Cet exemple utilise la notation `fileb://` pour transmettre le fichier d'objet d'événement. Il inclut également des sauts de ligne pour rendre la commande plus lisible.

```
aws cloudfront test-function \
    --name MaxAge \
    --if-match ETVABCEXAMPLE \
    --event-object fileb://event-maxage-test01.json \
    --stage DEVELOPMENT
```

> **Remarques**
>
> - Vous référencez la fonction par son nom et ETag (dans le `if-match` paramètre). Vous référencez l'objet d'événement par son emplacement dans votre système de fichiers.

- Il peut s'agir de la phase `DEVELOPMENT` ou `LIVE`.

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
TestResult:
  ComputeUtilization: '21'
  FunctionErrorMessage: ''
  FunctionExecutionLogs: []
  FunctionOutput: '{"response":{"headers":{"cloudfront-functions":
{"value":"generated-by-CloudFront-Functions"},"location":{"value":"https://
aws.amazon.com/cloudfront/"}},"statusDescription":"Found","cookies":
{},"statusCode":302}}'
  FunctionSummary:
    FunctionConfig:
      Comment: MaxAge function
      Runtime: cloudfront-js-2.0
      KeyValueStoreAssociations= \
      {Quantity=1, \
      Items=[{KeyValueStoreARN='arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111'}]} \
    FunctionMetadata:
      CreatedTime: '2021-04-18T20:38:56.915000+00:00'
      FunctionARN: arn:aws:cloudfront::111122223333:function/MaxAge
      LastModifiedTime: '2023-17-20T10:38:57.057000+00:00'
      Stage: DEVELOPMENT
    Name: MaxAge
    Status: UNPUBLISHED
```

Remarques

- `FunctionExecutionLogs` contient une liste de lignes de journaux que la fonction a écrites dans les instructions `console.log()` (le cas échéant).
- `ComputeUtilization` contient des informations sur l'exécution de votre fonction. Consultez the section called "Présentation de l'utilisation du calcul".
- `FunctionOutput` contient l'objet d'évènement renvoyé par la fonction.

Présentation de l’utilisation du calcul

L'utilisation du calcul est la durée d'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une valeur de 35 signifie que la durée d’exécution de la fonction représente 35 % du temps maximum autorisé.

Si une fonction dépasse continuellement la durée maximale autorisée CloudFront , elle ralentit. La liste suivante explique la probabilité qu'une fonction soit limitée en fonction de la valeur d'utilisation du calcul.

Valeur d'utilisation du calcul :

- 1 – 50 : la fonction est largement inférieure à la durée maximale autorisée et devrait s'exécuter sans aucune limitation.
- 51 – 70 : la fonction approche de la durée maximale autorisée. Pensez à optimiser le code de fonction.
- 71 — 100 — La durée maximale autorisée de la fonction est très proche ou supérieure. CloudFront est susceptible de limiter cette fonction si vous l'associez à une distribution.

Mise à jour de fonctions

Vous pouvez mettre à jour une fonction à tout moment. Les modifications sont apportées uniquement à la version de la fonction qui figure dans la phase `DEVELOPMENT`. Pour copier les mises à jour de la phase `DEVELOPMENT` vers `LIVE`, vous devez publier la fonction.

Vous pouvez mettre à jour le code d'une fonction dans la CloudFront console ou avec le AWS Command Line Interface (AWS CLI).

Console

Pour mettre à jour le code de la fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.

   Sélectionnez la fonction à mettre à jour.
2. Choisissez Modifier et apportez les modifications suivantes :

   - Mettez à jour tous les champs de la section Détails.

- Modifiez ou supprimez le magasin de clés-valeurs associé. Pour plus d'informations sur les magasins de clés-valeurs, consultez the section called " CloudFront KeyValueStore".

- Modifiez le code de la fonction. Choisissez l'onglet Création, apportez des modifications, puis sélectionnez Enregistrer les modifications pour enregistrer les modifications apportées au code.

CLI

Mettre à jour le code de la fonction.

1. Ouvrez une fenêtre de ligne de commande.
2. Exécutez la commande suivante.

   Cet exemple utilise la notation `fileb://` pour transmettre le fichier. Il inclut également des sauts de ligne pour rendre la commande plus lisible.

```
aws cloudfront update-function \
    --name MaxAge \
    --function-config '{"Comment":"Max Age 2 years","Runtime":"cloudfront-
js-2.0","KeyValueStoreAssociations":{"Quantity":1,"Items":
[{"KeyValueStoreARN":"arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"}]}}' \
    --function-code fileb://function-max-age-v1.js \
    --if-match ETVABCEXAMPLE
```

   Remarques

   - Vous pouvez identifier la fonction à la fois par son nom et ETag (dans le `if-match` paramètre). Assurez-vous d'utiliser le courant ETag. Vous pouvez obtenir cette valeur à partir de l'opération DescribeFunctiond'API.
   - Vous devez inclure l'élément `function-code`, même si vous ne voulez pas le modifier.
   - Soyez prudent avec l'élément `function-config`. Vous devez transmettre tout ce que vous voulez conserver dans la configuration. En particulier, gérez le magasin de clés-valeurs comme suit :

- Pour conserver l'association de magasin de clés-valeurs existante (le cas échéant), spécifiez le nom du magasin existant.
- Pour modifier l'association, spécifiez le nom du nouveau magasin de clés-valeurs.
- Pour supprimer l'association, omettez le paramètre `KeyValueStoreAssociations`.

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
ETag: ETVXYZEXAMPLE
FunctionSummary:
  FunctionConfig:
    Comment: Max Age 2 years \
    Runtime: cloudfront-js-2.0 \
    KeyValueStoreAssociations= \
      {Quantity=1, \
      Items=[{KeyValueStoreARN='arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111'}]} \
  FunctionMetadata: \
    CreatedTime: '2021-04-18T20:38:56.915000+00:00' \
    FunctionARN: arn:aws:cloudfront::111122223333:function/MaxAge \
    LastModifiedTime: '2023-12-19T23:41:15.389000+00:00' \
    Stage: DEVELOPMENT \
  Name: MaxAge \
  Status: UNPUBLISHED
```

La plupart des informations proviennent de la demande. D'autres informations sont ajoutées par CloudFront.

Remarques

- `ETag` : cette valeur change chaque fois que vous modifiez le magasin de clés-valeurs.
- `FunctionARN`— L'ARN de votre CloudFront fonction.
- `Stage` : le stade de la fonction (`LIVE` ou `DEVELOPMENT`).
- `Status` : l'état de la fonction (`PUBLISHED` ou `UNPUBLISHED`).

Publication de fonctions

Lorsque vous publiez votre fonction, celle-ci est copiée de l'étape `DEVELOPMENT` vers l'étape `LIVE`.

Si aucun comportement de cache n'est associé à la fonction, sa publication vous permet de l'associer à un comportement de cache. Vous pouvez uniquement associer des comportements de cache à des fonctions qui sont à l'étape `LIVE`.

> **Important**
>
> - Nous recommandons de tester la fonction avant de la publier.
> - Une fois la fonction publiée, tous les comportements de cache qui lui sont associés commencent automatiquement à utiliser la nouvelle copie publiée, dès que les distributions ont terminé leur déploiement.

Vous pouvez publier une fonction dans la console CloudFront ou avec AWS CLI.

Console

Pour publier une fonction

1. Connectez-vous à la console CloudFront à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Sélectionnez la fonction à mettre à jour.
3. Choisissez l'onglet Publier, puis sélectionnez Publier. Si votre fonction est déjà associée à un ou plusieurs comportements de cache, choisissez Publier et mettre à jour.
4. (Facultatif) Pour afficher les distributions associées à la fonction, choisissez Distributions CloudFront associées pour développer cette section.

En cas de réussite, une bannière apparaît en haut de la page avec le message : ***`Nom de la fonction`*** publié. Vous pouvez également choisir l'onglet Générer, puis Live pour afficher la version live du code de fonction.

CLI

Pour publier une fonction

1. Ouvrez une fenêtre de ligne de commande.

2. Exécutez la commande suivante aws cloudfront publish-function. Dans l'exemple, des sauts de ligne sont fournis pour rendre l'exemple plus lisible.

```
aws cloudfront publish-function \
    --name MaxAge \
    --if-match ETVXYZEXAMPLE
```

Lorsque la commande s'exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
FunctionSummary:
  FunctionConfig:
    Comment: Max Age 2 years
    Runtime: cloudfront-js-2.0
  FunctionMetadata:
    CreatedTime: '2021-04-18T21:24:21.314000+00:00'
    FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
    LastModifiedTime: '2023-12-19T23:41:15.389000+00:00'
    Stage: LIVE
  Name: MaxAge
  Status: UNASSOCIATED
```

Association de fonctions à des distributions

Pour utiliser une fonction avec une distribution, associez la fonction à un ou plusieurs comportements de cache dans la distribution. Vous pouvez associer une fonction à plusieurs comportements de cache dans plusieurs distributions.

Vous pouvez associer une fonction avec l'un des éléments suivants :

- Un comportement de cache existant
- Un nouveau comportement de cache dans une distribution existante
- Un nouveau comportement de cache dans une nouvelle distribution

Lorsque vous associez une fonction à un comportement de cache, vous devez choisir un type d'évènement. Le type d'évènement détermine quand CloudFront exécute la fonction.

Vous pouvez choisir parmi les types d'événement suivants :

- Demande utilisateur : la fonction s'exécute lorsque CloudFront reçoit une demande provenant d'un utilisateur.
- Réponse utilisateur – la fonction s'exécute avant que CloudFront ne renvoie une réponse à l'utilisateur.

Vous ne pouvez pas utiliser de types d'évènements orientés vers l'origine (requête d'origine et réponse d'origine) avec Fonctions CloudFront. Vous pouvez utiliser Lambda@Edge à la place. Pour plus d'informations, consultez CloudFront événements pouvant déclencher une fonction Lambda @Edge.

> **Note**
>
> Avant d'associer une fonction, vous devez la publier à l'étape `LIVE`.

Vous pouvez associer une fonction à une distribution dans la console CloudFront ou avec l'AWS Command Line Interface (AWS CLI). La procédure suivante montre comment associer une fonction à un comportement de cache existant.

Console

Pour associer une fonction à un comportement de cache existant

1. Connectez-vous à la console CloudFront à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Choisissez la fonction que vous souhaitez associer.
3. Sur la page Fonction, choisissez l'onglet Publier.
4. Choisissez Fonction Publier.
5. Choisissez Ajouter une association. Dans la boîte de dialogue qui apparaît, choisissez une distribution, un type d'événement et/ou un comportement de cache.

   Pour le type d'événement, choisissez le moment où vous souhaitez que cette fonction s'exécute :

   - Demande de l'utilisateur : exécute la fonction chaque fois que CloudFront reçoit une demande.

- Réponse de l'utilisateur : exécute la fonction chaque fois que CloudFront renvoie une réponse.

6. Pour enregistrer la configuration, choisissez Ajouter une association.

CloudFront associe la distribution à la fonction. Attendez quelques minutes pour que la distribution associée termine son déploiement. Vous pouvez choisir Afficher la distribution sur la page de détails de la fonction pour vérifier la progression.

CLI

Pour associer une fonction à un comportement de cache existant

1. Ouvrez une fenêtre de ligne de commande.
2. Saisissez la commande suivante pour enregistrer la configuration de distribution pour la distribution dont vous souhaitez associer le comportement de cache à une fonction. Cette commande enregistre la configuration de distribution dans un fichier nommé `dist-config.yaml`. Pour utiliser cette commande, procédez comme suit :

   - Remplacez *`DistributionID`* par l'ID de la distribution.
   - Exécutez la commande sur une ligne. Dans l'exemple, des sauts de ligne sont fournis pour rendre l'exemple plus lisible.

   ```
   aws cloudfront get-distribution-config \
       --id DistributionID \
       --output yaml > dist-config.yaml
   ```

   Lorsque la commande réussit, AWS CLI ne renvoie aucune sortie.

3. Ouvrez le fichier nommé `dist-config.yaml` que vous avez créé. Apportez les modifications suivantes au fichier.

   a. Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

   b. Dans le comportement du cache, recherchez l'objet nommé `FunctionAssociations`. Mettez à jour cet objet pour ajouter une association de fonctions. La syntaxe YAML pour une association de fonctions ressemble à l'exemple ci-dessous.

- L'exemple suivant montre un objet d'évènement de requête utilisateur (déclenchement). Pour utiliser le type d'évènement Réponse utilisateur, remplacez `viewer-request` par `viewer-response`.
- Remplacez *`arn:aws:cloudfront::111122223333:function/ExampleFunction`* par l'Amazon Resource Name (ARN) de la fonction que vous associez à ce comportement de cache. Pour obtenir l'ARN de la fonction, vous pouvez utiliser la commande aws cloudfront list-functions.

```
FunctionAssociations:
  Items:
    - EventType: viewer-request
      FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
  Quantity: 1
```

c. Après avoir effectué ces modifications, enregistrez le fichier.

4. Utilisez la commande suivante pour mettre à jour la distribution, en ajoutant l'association de fonctions. Pour utiliser cette commande, procédez comme suit :

- Remplacez *`DistributionID`* par l'ID de la distribution.
- Exécutez la commande sur une ligne. Dans l'exemple, des sauts de ligne sont fournis pour rendre l'exemple plus lisible.

```
aws cloudfront update-distribution \
    --id DistributionID \
    --cli-input-yaml file://dist-config.yaml
```

Lorsque la commande réussit, vous voyez une sortie similaire à la suivante, qui décrit la distribution qui vient d'être mise à jour avec l'association de fonctions. L'exemple de sortie suivant est tronqué pour plus de lisibilité.

```
Distribution:
  ARN: arn:aws:cloudfront::111122223333:distribution/EBEDLT3BGRBBW
  ... truncated ...
  DistributionConfig:
    ... truncated ...
    DefaultCacheBehavior:
      ... truncated ...
```

```
      FunctionAssociations:
        Items:
        - EventType: viewer-request
          FunctionARN: arn:aws:cloudfront::111122223333:function/ExampleFunction
        Quantity: 1
      ... truncated ...
  DomainName: d111111abcdef8.cloudfront.net
  Id: EDFDVBD6EXAMPLE
  LastModifiedTime: '2021-04-19T22:39:09.158000+00:00'
  Status: InProgress
ETag: E2VJGGQEG1JT8S
```

Le `Status` de la distribution passe à `InProgress` pendant le redéploiement de la distribution. Lorsque la nouvelle configuration de distribution atteint un emplacement périphérique CloudFront, cet emplacement commence à utiliser la fonction associée. Lorsque la distribution est entièrement déployée, l'`Status` repasse à `Deployed`. Cela indique que la fonction CloudFront associée est active dans l'ensemble des emplacements périphériques CloudFront dans le monde. Cela prend généralement quelques minutes.

Amazon CloudFront KeyValueStore

CloudFront KeyValueStore est une banque de données de valeurs clés sécurisée, globale et à faible latence qui permet un accès en lecture depuis CloudFront Functions, permettant ainsi une logique personnalisable avancée aux emplacements CloudFront périphériques.

Vous pouvez ainsi mettre à jour le code de fonction et les données associées à une fonction indépendamment les unes des autres. CloudFront KeyValueStore Cette séparation simplifie le code des fonctions et facilite la mise à jour des données sans qu'il soit nécessaire de déployer des modifications de code.

> **Note**
>
> Pour être utilisée CloudFront KeyValueStore, votre CloudFront fonction doit utiliser le JavaScript runtime 2.0.

La procédure générale d'utilisation des paires clé-valeur est la suivante :

- Créez un magasin de clés-valeurs et remplissez-le avec un ensemble de paires clé-valeur. Vous pouvez ajouter vos magasins de clés-valeurs à un compartiment Amazon S3 ou les saisir manuellement.
- Associez les magasins de valeurs clés à votre CloudFront fonction.
- Dans votre code de fonction, utilisez le nom de la clé pour extraire la valeur associée à la clé ou pour évaluer si une clé existe. Pour plus d'informations sur l'utilisation de paires clé-valeur dans le code de fonction, ainsi que sur les méthodes d'assistance, consultez the section called "Méthodes d'aide pour les magasins de clés-valeurs".

Cas d'utilisation

Vous pouvez utiliser des paires clé-valeur pour les exemples suivants :

- Réécritures ou redirections d'URL : la paire clé-valeur peut contenir la réécriture ou la redirection URLs . URLs
- Tests A/B et indicateurs de fonctionnalités : vous pouvez créer une fonction pour effectuer des tests en attribuant un pourcentage de trafic à une version spécifique de votre site web.
- Autorisation d'accès : vous pouvez implémenter un contrôle d'accès pour autoriser ou refuser les demandes en fonction de critères que vous avez définis et des données stockées dans un magasin de clés-valeurs.

Formats de valeurs pris en charge

Vous pouvez stocker la valeur d'une paire clé-valeur dans l'un des formats suivants :

- String
- Chaîne codée en octets
- JSON

Sécurité

La CloudFront fonction et toutes ses valeurs clés stockent les données sont traitées de manière sécurisée, comme suit :

- CloudFront chiffre chaque valeur clé stockée au repos et pendant le transit (lors de la lecture ou de l'écriture dans les magasins de valeurs clés) lorsque vous appelez les opérations de l'CloudFront KeyValueStoreAPI.
- Lorsque la fonction est exécutée, CloudFront déchiffre chaque paire clé-valeur en mémoire aux emplacements périphériques. CloudFront

Pour commencer CloudFront KeyValueStore, consultez les rubriques suivantes.

Rubriques

- Utilisation de magasins de clés-valeurs
- Utilisation de données clé-valeur

- Pour plus d'informations sur la mise en route CloudFront KeyValueStore, consultez le billet de CloudFront KeyValueStore AWS blog « Présentation d'Amazon ».

Utilisation de magasins de clés-valeurs

Vous devez créer un magasin clé-valeur pour contenir les paires clé-valeur que vous souhaitez utiliser dans CloudFront Functions.

Après avoir créé les magasins de valeurs clés et les paires clé-valeur ajoutées, vous pouvez utiliser les valeurs clés dans votre code de CloudFront fonction.

Pour commencer, consultez les rubriques suivantes :

Rubriques

- Création d’un magasin de clés-valeurs
- Association d’un magasin de clés-valeurs à une fonction
- Mise à jour d’un magasin de clés-valeurs
- Obtention d’une référence à un magasin de clés-valeurs
- Suppression d’un magasin de clés-valeurs
- Format de fichier pour les paires clé-valeur

> **Note**
>
> Le JavaScript runtime 2.0 inclut des méthodes d'assistance pour travailler avec des valeurs clés dans le code de fonction. Pour de plus amples informations, veuillez consulter the section called “Méthodes d’aide pour les magasins de clés-valeurs”.

Création d’un magasin de clés-valeurs

Vous pouvez créer un magasin de clés-valeurs et ses paires clé-valeur en même temps. Vous pouvez également créer un magasin de clés-valeurs vide, puis ajouter des paires clé-valeur ultérieurement.

> **Note**
>
> Si vous spécifiez votre source de données à partir d’un compartiment Amazon S3, vous devez disposer des autorisations `s3:GetObject` et `s3:GetBucketLocation` pour ce compartiment. Si vous ne disposez pas de ces autorisations, vous ne CloudFront pourrez pas créer correctement votre magasin de valeurs clés.

Décidez si vous souhaitez ajouter des paires clé-valeur en même temps que vous créez le magasin de clés-valeurs. Vous pouvez importer vos paires clé-valeur à l'aide de la CloudFront console, de l' CloudFrontAPI ou. AWS SDKs Toutefois, vous ne pouvez importer votre fichier de paires clé-valeur que lorsque vous créez initialement le magasin de clés-valeurs.

Pour créer un fichier de paires clé-valeur, consultez Format de fichier pour les paires clé-valeur.

Console

Pour créer un magasin de clés-valeurs

1. Connectez-vous à la page Fonctions Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Choisissez l'KeyValueStoresonglet, puis sélectionnez Créer KeyValueStore.
3. Entrez un nom et une description facultative pour le magasin de clés-valeurs.

4. Complétez URI S3 :

   - Si vous disposez d'un fichier de paires clé-valeur, entrez le chemin d'accès au compartiment Amazon S3 où vous avez stocké le fichier.
   - Laissez ce champ vide si vous prévoyez d'entrer manuellement les paires clé-valeur.

5. Choisissez Créer. Le magasin de clés-valeurs existe désormais.

   La page de détails du nouveau magasin de clés-valeurs apparaît. Les informations figurant sur cette page incluent l'ID et l'ARN du magasin de clés-valeurs.

   - L'identifiant est une chaîne de caractères aléatoire unique dans votre Compte AWS.
   - La syntaxe de l'ARN est la suivante :

     Compte AWS:key-value-store/*the key value stores ID*

6. Examinez la section Paires clé-valeur. Si vous avez importé un fichier, cette section présente quelques paires clé-valeur. Vous pouvez effectuer les opérations suivantes :

   - Si vous avez importé un fichier, vous pouvez également ajouter d'autres valeurs manuellement.
   - Si vous n'avez pas importé de fichier d'un compartiment Amazon S3 et si vous souhaitez ajouter des paires clé-valeur dès maintenant, vous pouvez passer à l'étape suivante.
   - Vous pouvez ignorer cette étape et ajouter les paires clé-valeur ultérieurement.

7. Pour ajouter les paires dès maintenant :

   a. Choisissez Ajouter des paires clé-valeur.

   b. Choisissez Ajouter une paire et entrez un nom et une valeur. Répétez cette étape pour ajouter d'autres paires.

   c. Lorsque vous avez terminé, choisissez Enregistrer les modifications pour enregistrer toutes les paires clé-valeur dans le magasin de clés-valeurs. Dans la boîte de dialogue qui s'affiche, cliquez sur Terminé.

8. Pour associer le magasin de clés-valeurs à une fonction dès maintenant, complétez la section Fonctions associées. Pour plus d'informations, consultez ??? ou ???.

   Vous pouvez également associer la fonction ultérieurement, soit depuis la page de détails de ce magasin de clés-valeurs, soit depuis la page de détails de la fonction.

AWS CLI

Pour créer un magasin de clés-valeurs

- Exécutez la commande suivante pour créer un magasin de clés-valeurs et importer les paires clé-valeur depuis un compartiment Amazon S3.

```
aws cloudfront create-key-value-store \
    --name=keyvaluestore1 \
    --comment="This is my key value store file" \
    --import-source=SourceType=S3,SourceARN=arn:aws:s3:::amzn-s3-demo-
bucket1/kvs-input.json
```

Réponse

```
{
    "ETag": "ETVABCEXAMPLE",
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/key-value-store/
arn:aws:cloudfront::123456789012:key-value-store/8aa76c93-3198-462c-aaf6-
example",
    "KeyValueStore": {
        "Name": "keyvaluestore1",
        "Id": "8aa76c93-3198-462c-aaf6-example",
        "Comment": "This is my key value store file",
        "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
        "Status": "PROVISIONING",
        "LastModifiedTime": "2024-08-06T22:19:10.813000+00:00"
    }
}
```

API

Pour créer un magasin de clés-valeurs

1. Utilisez l'CloudFrontCreateKeyValueStoreopération. L'opération prend plusieurs paramètres :
   - Un `name` du magasin de clés-valeurs.
   - Un paramètre `comment` qui inclut un commentaire.
   - Un paramètre `import-source` qui vous permet d'importer des paires clé-valeur à partir d'un fichier stocké dans un compartiment Amazon S3. Vous ne pouvez importer à partir

d'un fichier qu'au moment de la création initiale du magasin de clés-valeurs. Pour plus d'informations sur la structure, consultez the section called "Format de fichier pour les paires clé-valeur".

La réponse de l'opération inclut les informations suivantes :

- Les valeurs transmises dans la demande, y compris le nom que vous avez attribué.
- Des données telles que l'heure de création.
- Un `ETag` (par exemple, `ETVABCEXAMPLE`), l'ARN qui inclut le nom du magasin de clés-valeurs (par exemple, `arn:aws:cloudfront::123456789012:key-value-store/keyvaluestore1`).

  Vous utiliserez une combinaison de l'`ETag`, de l'ARN et du nom pour travailler avec le magasin de clés-valeurs par programmation.

États des magasins de clés-valeurs

Lorsque vous créez un magasin de clés-valeurs, le magasin de données peut présenter les valeurs d'état suivantes.

Value	Description
Approvisionnement	Le magasin de valeurs clés a été créé et CloudFront traite la source de données que vous avez spécifiée.
Prêt	Le magasin de valeurs clés a été créé et a traité CloudFront avec succès la source de données que vous avez spécifiée.
Échec de l'importation	CloudFront n'a pas pu traiter la source de données que vous avez spécifiée . Cet état peut apparaître si le format de votre fichier n'est pas valide ou s'il dépasse la limite de taille. Pour de plus amples informations, veuillez consulter Format de fichier pour les paires clé-valeur.

Association d’un magasin de clés-valeurs à une fonction

Après avoir créé votre magasin de clés-valeurs, vous pouvez mettre à jour votre fonction pour l’associer à votre magasin de clés-valeurs. Vous devez établir cette association pour pouvoir utiliser les paires clé-valeur de ce magasin dans cette fonction. Les règles suivantes s’appliquent :

- Une fonction peut avoir un seul magasin de clés-valeurs
- Vous pouvez associer le même magasin de clés-valeurs à plusieurs fonctions

Console

Pour associer un magasin de clés-valeurs à une fonction

1. Connectez-vous à la CloudFront console à l'adresse https://console.aws.amazon.com/cloudfront/v4/home#/functions et sélectionnez la page Fonctions.
2. Choisissez le nom de la fonction.
3. Accédez à la KeyValueStore section Associer et choisissez Associer existant KeyValueStore.
4. Sélectionnez le magasin clé-valeur qui contient les paires clé-valeur de la fonction, puis choisissez Associer. KeyValueStore

   CloudFront associe immédiatement le magasin à la fonction. Vous n’avez pas besoin d’enregistrer la fonction.
5. Pour spécifier un autre magasin de valeurs clés, choisissez Mettre à jour associé KeyValueStore, sélectionnez un autre nom de magasin de valeurs clés, puis choisissez Associer KeyValueStore.

Pour de plus amples informations, veuillez consulter the section called “Mise à jour de fonctions”.

AWS CLI

Pour associer un magasin de clés-valeurs à une fonction

- Exécutez la commande suivante pour mettre à jour la fonction *MaxAge* et associer une ressource de magasin de clés-valeurs.

```
aws cloudfront update-function \
    --name MaxAge \
    --function-config '{"Comment":"Max Age 2 years","Runtime":"cloudfront-
js-2.0","KeyValueStoreAssociations":{"Quantity":1,"Items":
```

```
[{"KeyValueStoreARN":"arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example"}]}}' \
    --function-code fileb://function-max-age-v1.js \
    --if-match ETVABCEXAMPLE
```

- Pour associer un magasin de clés-valeurs à une fonction, spécifiez le paramètre `KeyValueStoreAssociations` et l'ARN du magasin de clés-valeurs.
- Pour modifier l'association, spécifiez un autre ARN de magasin de clés-valeurs.
- Pour supprimer l'association, supprimez le paramètre `KeyValueStoreAssociations`.

Pour de plus amples informations, veuillez consulter the section called "Mise à jour de fonctions".

API

Pour associer un magasin de clés-valeurs à une fonction

- Utilisez l'opération d'API UpdateFunction. Pour de plus amples informations, veuillez consulter the section called "Mise à jour de fonctions".

> **Remarques**
>
> - Si vous modifiez un magasin de clés-valeurs sans modifier les paires clé-valeur, ou si vous ne modifiez que les paires clé-valeur dans le magasin, vous n'avez pas besoin d'associer de nouveau le magasin de clés-valeurs. Vous n'avez pas non plus besoin de republier la fonction.
>
> Toutefois, nous vous recommandons de tester la fonction afin de vérifier qu'elle fonctionne comme prévu. Pour de plus amples informations, veuillez consulter Fonctions de test.
> - Vous pouvez afficher toutes les fonctions qui utilisent des magasins de clés-valeurs spécifiques. Sur la CloudFront console, choisissez la page de détails du magasin de valeurs clés.

Mise à jour d'un magasin de clés-valeurs

Lorsque vous mettez à jour un magasin de clés-valeurs, vous pouvez modifier les paires clé-valeur ou modifier l'association entre le magasin de clés-valeurs et la fonction.

Console

Pour mettre à jour un magasin de clés-valeurs

1. Connectez-vous à la page Fonctions Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Cliquez sur l'onglet KeyValueStores.
3. Sélectionnez le magasin de clés-valeurs que vous souhaitez mettre à jour.
   - Pour mettre à jour les paires clé-valeur, choisissez Modifier dans la section Paires clé-valeur. Vous pouvez ajouter ou supprimer n'importe quelle paire clé-valeur. Vous pouvez également modifier la valeur d'une paire clé-valeur existante. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.
   - Pour mettre à jour l'association pour ce magasin de clés-valeurs, choisissez Accéder aux fonctions. Pour de plus amples informations, veuillez consulter the section called "Association d'un magasin de clés-valeurs à une fonction".

AWS CLI

Pour mettre à jour un magasin de clés-valeurs

1. Modifier les paires clé-valeur : vous pouvez ajouter d'autres paires clé-valeur, supprimer une ou plusieurs paires clé-valeur et modifier la valeur d'une paire clé-valeur existante. Pour de plus amples informations, veuillez consulter Utilisation de données clé-valeur.
2. Modifier l'association de la fonction pour le magasin de clés-valeurs : pour mettre à jour l'association de la fonction pour le magasin de clés-valeurs, consultez Association d'un magasin de clés-valeurs à une fonction.

> **Tip**
>
> Vous aurez besoin de l'ARN du magasin de clés-valeurs. Pour de plus amples informations, veuillez consulter the section called "Obtention d'une référence à un magasin de clés-valeurs".

API

Pour mettre à jour un magasin de clés-valeurs

1. Modifier les paires clé-valeur : vous pouvez ajouter d'autres paires clé-valeur, supprimer une ou plusieurs paires clé-valeur et modifier la valeur d'une paire clé-valeur existante. Pour de plus amples informations, veuillez consulter Utilisation de données clé-valeur.
2. Modifier l'association de fonction pour le magasin de valeurs clés : pour mettre à jour l'association de fonctions pour le magasin de valeurs clés, utilisez l'opération UpdateFunctionAPI. Pour de plus amples informations, veuillez consulter the section called "Mise à jour de fonctions".

> **Tip**
>
> Vous aurez besoin de l'ARN du magasin de clés-valeurs. Pour de plus amples informations, veuillez consulter the section called "Obtention d'une référence à un magasin de clés-valeurs".

Obtention d'une référence à un magasin de clés-valeurs

Pour utiliser le magasin de clés-valeurs par programmation, vous avez besoin de l'`ETag` et du nom du magasin de clés-valeurs.

Pour obtenir les deux valeurs, vous pouvez utiliser le AWS Command Line Interface (AWS CLI) ou l' CloudFront API.

AWS CLI

Pour obtenir la référence à un magasin de clés-valeurs

1. Pour renvoyer une liste des magasins de clés-valeurs, exécutez la commande suivante. Recherchez ensuite le nom du magasin de clés-valeurs que vous souhaitez modifier.

```
aws cloudfront list-key-value-stores
```

2. Dans la réponse, recherchez le nom du magasin de clés-valeurs souhaité.

   Réponse

```
{
    "KeyValueStoreList": {
        "Items": [
            {
                "Name": "keyvaluestore3",
                "Id": "37435e19-c205-4271-9e5c-example3",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/37435e19-c205-4271-9e5c-example3",
                "Status": "READY",
                "LastModifiedTime": "2024-05-08T14:50:18.876000+00:00"
            },
            {
                "Name": "keyvaluestore2",
                "Id": "47970d59-6408-474d-b850-example2",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/47970d59-6408-474d-b850-example2",
                "Status": "READY",
                "LastModifiedTime": "2024-05-30T21:06:22.113000+00:00"
            },
            {
                "Name": "keyvaluestore1",
                "Id": "8aa76c93-3198-462c-aaf6-example",
                "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
                "Status": "READY",
                "LastModifiedTime": "2024-08-06T22:19:30.510000+00:00"
            }
        ]
    }
}
```

3. Exécutez la commande suivante pour renvoyer l'`ETag` du magasin de clés-valeurs spécifié.

```
aws cloudfront describe-key-value-store \
    --name=keyvaluestore1
```

Réponse

```
{
    "ETag": "E3UN6WX5RRO2AG",
    "KeyValueStore": {
        "Name": "keyvaluestore1",
```

```
        "Id": "8aa76c93-3198-462c-aaf6-example",
        "Comment": "This is an example KVS",
        "ARN": "arn:aws:cloudfront::123456789012:key-value-
store/8aa76c93-3198-462c-aaf6-example",
        "Status": "READY",
        "LastModifiedTime": "2024-08-06T22:19:30.510000+00:00"
    }
}
```

API

Pour obtenir la référence à un magasin de clés-valeurs

1. Utilisez l'opération d'API CloudFront ListKeyValueStores pour renvoyer une liste de magasins de clés-valeurs. Recherchez le nom du magasin de clés-valeurs que vous souhaitez modifier.
2. Utilisez l'opération d'API CloudFront DescribeKeyValueStore et indiquez le nom du magasin de clés-valeurs que vous avez renvoyé à l'étape précédente.

La réponse inclut un UUID, l'ARN du magasin de clés-valeurs et l'`ETag` du magasin de clés-valeurs.

- Un `ETag`, par exemple `E3UN6WX5RRO2AG`
- L'UUID est de 128 bits, tel que `8aa76c93-3198-462c-aaf6-example`
- L'ARN inclut le Compte AWS nombre, la constante `key-value-store` et l'UUID, comme dans l'exemple suivant :

  `arn:aws:cloudfront::123456789012:key-value-store/8aa76c93-3198-462c-aaf6-example`

Pour plus d'informations sur l'opération `DescribeKeyValueStore`, consultez the section called "À propos de CloudFront KeyValueStore".

Suppression d'un magasin de clés-valeurs

Vous pouvez supprimer votre boutique de valeurs clés à l'aide de la CloudFront console ou de l'API Amazon.

Console

Pour supprimer un magasin de clés-valeurs

1. Connectez-vous à la page Fonctions Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Choisissez le nom de la fonction.
3. Dans la KeyValueStore section Associé, vérifiez si un magasin de valeurs clés est associé à la fonction. Si tel est le cas, supprimez l'association en choisissant Dissocier, KeyValueStore puis en choisissant Supprimer l'association.
4. Dans le volet de navigation, choisissez la page Fonctions, puis sélectionnez l'KeyValueStoresonglet.
5. Sélectionnez le magasin de clés-valeurs que vous souhaitez supprimer, puis choisissez Supprimer.

AWS CLI

Pour supprimer un magasin de clés-valeurs

1. Obtenez l'`ETag` et le nom du magasin de clés-valeurs. Pour de plus amples informations, veuillez consulter the section called "Obtention d'une référence à un magasin de clés-valeurs".
2. Vérifiez si le magasin de clés-valeurs est associé à une fonction. S'il l'est, supprimez l'association. Pour plus d'informations sur ces étapes, consultez ???.
3. Une fois que vous disposez du nom et de l'`ETag` du magasin clé-valeur et qu'il n'est plus associé à une fonction, vous pouvez le supprimer.

   Exécutez la commande suivante pour supprimer le magasin de clés-valeurs spécifié.

   ```
   aws cloudfront delete-key-value-store \
       --name=keyvaluestore1 \
       --if-match=E3UN6WX5RRO2AG
   ```

API

Pour supprimer un magasin de clés-valeurs

1. Obtenez l'ETag et le nom du magasin de clés-valeurs. Pour de plus amples informations, veuillez consulter the section called "Obtention d'une référence à un magasin de clés-valeurs".
2. Vérifiez si le magasin de clés-valeurs est associé à une fonction. S'il l'est, supprimez l'association. Pour plus d'informations sur ces étapes, consultez ???.
3. Pour supprimer le magasin de valeurs clés, utilisez l'opération CloudFront DeleteKeyValueStoreAPI.

Format de fichier pour les paires clé-valeur

Lorsque vous créez un fichier codé en UTF-8, utilisez le format JSON suivant :

```
{
  "data":[
    {
      "key":"key1",
      "value":"value"
    },
    {
      "key":"key2",
      "value":"value"
    }
  ]
}
```

Votre fichier ne peut pas inclure de clés en double. Si vous avez indiqué un fichier invalide dans votre compartiment Amazon S3, vous pouvez mettre le fichier à jour pour supprimer les doublons, puis réessayer de créer votre magasin de clés-valeurs.

Pour de plus amples informations, veuillez consulter Création d'un magasin de clés-valeurs.

> **Note**
>
> Le fichier de votre source de données et ses paires clé-valeur présentent les limites suivantes :

- Taille du fichier : 5 Mo
- Taille de la clé : 512 caractères
- Taille de la valeur : 1024 caractères

Utilisation de données clé-valeur

Cette rubrique décrit comment ajouter des paires clé-valeur à un magasin de clés-valeurs existant. Pour inclure des paires clé-valeur lorsque vous créez initialement le magasin de clés-valeurs, consultez the section called “Création d’un magasin de clés-valeurs”.

Rubriques

- Utilisation de paires clé-valeur (console)
- À propos de CloudFront KeyValueStore
- Utilisation des paires clé-valeur (AWS CLI)
- Utilisation des paires clé-valeur (API)

Utilisation de paires clé-valeur (console)

Vous pouvez utiliser la CloudFront console pour travailler avec vos paires clé-valeur.

Pour utiliser les paires clé-valeur

1. Connectez-vous à la page Fonctions Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home#/functions.
2. Cliquez sur l'onglet KeyValueStores.
3. Sélectionnez le magasin de clés-valeurs que vous souhaitez modifier.
4. Dans la section Paires clé-valeur, choisissez Modifier.
5. Vous pouvez ajouter une paire clé-valeur, supprimer une paire clé-valeur ou modifier la valeur d’une paire clé-valeur existante.
6. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

À propos de CloudFront KeyValueStore

> **Tip**
>
> L' CloudFront KeyValueStore API est un service mondial qui utilise Signature Version 4A (SigV4A) pour l'authentification. L'utilisation d'informations d'identification temporaires avec SigV4A nécessite des jetons de session de version 2. Pour de plus amples informations, veuillez consulter Utilisation d'informations d'identification temporaires avec l' CloudFront KeyValueStore API.

Si vous utilisez le AWS Command Line Interface (AWS CLI) ou votre propre code pour appeler l' CloudFront KeyValueStore API, consultez les sections suivantes.

Lorsque vous utilisez un magasin de clés-valeurs et ses paires clé-valeur, le service que vous appelez dépend de votre cas d'utilisation :

- Pour utiliser des paires clé-valeur dans un magasin clé-valeur existant, utilisez le CloudFront KeyValueStore service.
- Pour inclure des paires clé-valeur dans le magasin clé-valeur lorsque vous créez initialement le magasin clé-valeur, utilisez le CloudFront service.

L' CloudFront API et l' CloudFront KeyValueStore API fonctionnent toutes deux. `DescribeKeyValueStore` Vous les appelez pour différentes raisons. Pour comprendre les différences, consultez le tableau suivant.

	API CloudFront DescribeKeyValueStore	API CloudFront KeyValueStore DescribeKeyValueStore
Données relatives au magasin de clés-valeurs	Renvoie des données, telles que l'état et la date à laquelle le magasin de clés-valeurs lui-même a été modifié pour la dernière fois.	Renvoie les données relatives au contenu de la ressource de stockage : les paires clé-valeur figurant dans le magasin et la taille du contenu.

	API CloudFront DescribeKeyValueStore	API CloudFront KeyValueStore DescribeKeyValueStore
Données qui identifient le magasin de clés-valeurs	Renvoie un ETag, l'UUID et l'ARN du magasin de clés-valeurs.	Renvoie un ETag et l'ARN du magasin de clés-valeurs.

Remarques

- Chaque opération DescribeKeyValueStore renvoie un ETag différent. Les ETags ne sont pas interchangeables.
- Lorsque vous appelez une opération d'API pour effectuer une action, vous devez spécifier l'ETag provenant de l'API appropriée. Par exemple, dans l' CloudFront KeyValueStore DeleteKeyopération, vous spécifiez ETag ce que vous avez renvoyé après l' CloudFront KeyValueStore DescribeKeyValueStoreopération.
- Lorsque vous appelez vos CloudFront fonctions en utilisant CloudFront KeyValueStore, les valeurs du magasin de valeurs clés ne sont ni mises à jour ni modifiées lors de l'appel de la fonction. Les mises à jour sont traitées entre deux invocations d'une fonction.

Utilisation des paires clé-valeur (AWS CLI)

Vous pouvez exécuter les AWS Command Line Interface commandes suivantes pour CloudFront KeyValueStore.

Table des matières

- Liste des paires clé-valeur
- Obtention des paires clé-valeur
- Description d'un magasin de clés-valeurs
- Création d'une paire clé-valeur
- Suppression d'une paire clé-valeur
- Mise à jour d'une paire clé-valeur

Liste des paires clé-valeur

Pour répertorier les paires clé-valeur dans votre magasin de clés-valeurs, exécutez la commande suivante.

```
aws cloudfront-keyvaluestore list-keys \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Réponse

```
{
    "Items": [
        {
            "Key": "key1",
            "Value": "value1"
        }
    ]
}
```

Obtention des paires clé-valeur

Pour obtenir les paires clé-valeur dans votre magasin de clés-valeurs, exécutez la commande suivante.

```
aws cloudfront-keyvaluestore get-key \
    --key=key1 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Réponse

```
{
    "Key": "key1",
    "Value": "value1",
    "ItemCount": 1,
    "TotalSizeInBytes": 11
}
```

Description d’un magasin de clés-valeurs

Pour décrire un magasin de clés-valeurs, exécutez la commande suivante.

```
aws cloudfront-keyvaluestore describe-key-value-store \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Réponse

```
{
    "ETag": "KV1F83G8C2ARO7P",
    "ItemCount": 1,
    "TotalSizeInBytes": 11,
    "KvsARN": "arn:aws:cloudfront::123456789012:key-value-store/37435e19-
c205-4271-9e5c-example",
    "Created": "2024-05-08T07:48:45.381000-07:00",
    "LastModified": "2024-08-05T13:50:58.843000-07:00",
    "Status": "READY"
}
```

Création d'une paire clé-valeur

Pour créer une paire clé-valeur dans votre magasin de clés-valeurs, exécutez la commande suivante.

```
aws cloudfront-keyvaluestore put-key \
    --if-match=KV1PA6795UKMFR9 \
    --key=key2 \
    --value=value2 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Réponse

```
{
    "ETag": "KV13V1IB3VIYZZH",
    "ItemCount": 3,
    "TotalSizeInBytes": 31
}
```

Suppression d'une paire clé-valeur

Pour supprimer une paire clé-valeur, exécutez la commande suivante.

```
aws cloudfront-keyvaluestore delete-key \
```

```
    --if-match=KV13V1IB3VIYZZH \
    --key=key1 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example
```

Sortie

```
{
    "ETag": "KV1VC38T7YXB528",
    "ItemCount": 2,
    "TotalSizeInBytes": 22
}
```

Mise à jour d'une paire clé-valeur

Vous pouvez utiliser la commande `update-keys` pour mettre à jour plusieurs paires clé-valeur. Par exemple, pour supprimer une paire clé-valeur existante et en créer une autre, exécutez la commande suivante.

```
aws cloudfront-keyvaluestore update-keys \
    --if-match=KV2EUQ1WTGCTBG2 \
    --kvs-arn=arn:aws:cloudfront::123456789012:key-value-store/37435e19-c205-4271-9e5c-
example \
    --deletes '[{"Key":"key2"}]' \
    --puts '[{"Key":"key3","Value":"value3"}]'
```

Réponse

```
{
    "ETag": "KV3AEGXETSR30VB",
    "ItemCount": 3,
    "TotalSizeInBytes": 28
}
```

Utilisation des paires clé-valeur (API)

Suivez cette section pour utiliser vos paires clé-valeur par programmation.

Table des matières

- Obtention d'une référence à un magasin de clés-valeurs

- Modification de paires clé-valeur dans un magasin de clés-valeurs
- Exemple de code pour CloudFront KeyValueStore

Obtention d'une référence à un magasin de clés-valeurs

Lorsque vous utilisez l' CloudFront KeyValueStore API pour appeler une opération d'écriture, vous devez spécifier l'ARN et le `ETag` du magasin de valeurs clés. Pour obtenir ces données, procédez comme suit :

Pour obtenir une référence à un magasin de clés-valeurs

1. Utilisez l'opération d'API CloudFront ListKeyValueStores pour obtenir une liste de magasins de clés-valeurs. Recherchez le magasin de clés-valeurs que vous souhaitez modifier.
2. Utilisez l'opération d'API CloudFrontKeyValueStore DescribeKeyValueStore et indiquez le magasin de clés-valeurs identifié à l'étape précédente.

   La réponse inclut l'ARN et l'`ETag` du magasin de clés-valeurs.

   - L'ARN inclut le Compte AWS nombre, la constante `key-value-store` et l'UUID, comme dans l'exemple suivant :

     ```
     arn:aws:cloudfront::123456789012:key-value-store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
     ```

   - Un `ETag` ressemble à l'exemple suivant :

     ```
     ETVABCEXAMPLE2
     ```

Modification de paires clé-valeur dans un magasin de clés-valeurs

Vous pouvez spécifier le magasin de clés-valeurs qui contient la paire clé-valeur que vous souhaitez mettre à jour.

Consultez les opérations CloudFront KeyValueStore d'API suivantes :

- CloudFrontKeyValueStore DeleteKey— Supprime une paire clé-valeur
- CloudFrontKeyValueStore GetKey— Renvoie une paire clé-valeur
- CloudFrontKeyValueStore ListKeys— Renvoie une liste de paires clé-valeur
- CloudFrontKeyValueStore PutKey— Vous pouvez effectuer les tâches suivantes :

  - Créer une paire clé-valeur dans un magasin de clés-valeurs en indiquant un nouveau nom de clé et une valeur.
  - Définir une valeur différente dans une paire clé-valeur existante en spécifiant un nom de clé existant et une nouvelle valeur.
- CloudFrontKeyValueStore UpdateKeys— Vous pouvez effectuer une ou plusieurs des actions suivantes en une seule all-or-nothing opération :
  - Supprimer une ou plusieurs paires clé-valeur
  - Créer une ou plusieurs nouvelles paires clé-valeur
  - Définir une valeur différente dans une ou plusieurs paires clé-valeur existantes

Exemple de code pour CloudFront KeyValueStore

Example

Le code suivant vous montre comment appeler l'opération d'API `DescribeKeyValueStore` pour un magasin de clés-valeurs.

```
const {
  CloudFrontKeyValueStoreClient,
  DescribeKeyValueStoreCommand,
} = require("@aws-sdk/client-cloudfront-keyvaluestore");

require("@aws-sdk/signature-v4-crt");

(async () => {
  try {
    const client = new CloudFrontKeyValueStoreClient({
      region: "us-east-1"
    });
    const input = {
      KvsARN: "arn:aws:cloudfront::123456789012:key-value-store/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
    };
    const command = new DescribeKeyValueStoreCommand(input);

    const response = await client.send(command);
  } catch (e) {
    console.log(e);
  }
```

```
})();
```

Personnalisez avec les fonctions CloudFront de connexion

CloudFront Les fonctions de connexion vous permettent d'écrire des JavaScript fonctions légères pour la validation des certificats mTLS et une logique d'authentification personnalisée. Vos fonctions de connexion s'exécutent lors de l'établissement de la connexion mTLS pour valider les certificats clients, implémenter des règles d'authentification spécifiques à l'appareil et gérer les scénarios de révocation de certificats. L'environnement d'exécution Connection Functions offre des temps de démarrage inférieurs à la milliseconde, s'adapte immédiatement pour gérer des millions de connexions par seconde et est hautement sécurisé. Les fonctions de connexion sont une fonctionnalité native de CloudFront, ce qui signifie que vous pouvez créer, tester et déployer votre code entièrement dans CloudFront.

Lorsque vous associez une fonction de connexion à une TLS-enabled CloudFront distribution m, CloudFront intercepte les demandes de connexion TLS aux emplacements CloudFront périphériques et transmet les informations de certificat à votre fonction. Vous pouvez appeler Connection Functions lorsque l'événement suivant se produit :

- Pendant l'établissement de la connexion TLS (demande de connexion) - pour les connexions TLS mutuelles (mTLS)

Pour plus d'informations sur les fonctions de connexion, consultez les rubriques suivantes.

Rubriques

- Vue d'ensemble et flux de travail
- Configuration et limites
- Création de fonctions de CloudFront connexion pour une validation mutuelle du protocole TLS (afficheur)
- Écrire le code de la fonction de CloudFront connexion pour la validation mutuelle du protocole TLS (afficheur)
- Testez les fonctions de CloudFront connexion avant le déploiement
- Associer les fonctions de connexion aux distributions
- Implémentez la révocation des certificats pour le TLS mutuel (visualiseur) avec CloudFront Functions et KeyValueStore

Vue d'ensemble et flux de travail

CloudFront Les fonctions de connexion sont un type spécialisé de CloudFront fonctions qui s'exécutent lors de la prise de contact TLS lorsqu'un client tente d'établir une connexion mTLS. Votre fonction de connexion peut accéder aux informations du certificat client, aux paramètres de configuration mTLS, aux résultats de la vérification de la révocation des certificats et à l'adresse IP du client.

Les fonctions de connexion sont invoquées après CloudFront avoir effectué la validation standard du certificat (chaîne de confiance, expiration, vérification de signature) mais peuvent être exécutées même si les contrôles de révocation des certificats échouent. Vous pouvez ainsi implémenter une logique personnalisée pour gérer les certificats révoqués ou ajouter des critères de validation supplémentaires.

Après avoir créé et publié une fonction de connexion, assurez-vous d'ajouter une association pour le type d'événement de demande de connexion avec une TLS-enabled distribution m. Cela permet à la fonction de s'exécuter chaque fois qu'un client tente d'établir une connexion mTLS avec CloudFront.

CloudFront Les fonctions de connexion suivent un cycle de vie en deux étapes que vous pouvez utiliser pour développer et tester des fonctions avant de les déployer en production. Ce flux de travail garantit que vos fonctions de connexion fonctionnent correctement avant qu'elles n'affectent le trafic réel.

Rubriques

- Étapes fonctionnelles
- Flux de travail du développement
- Différences par rapport aux autres types de fonctions

Étapes fonctionnelles

Les fonctions de connexion existent en deux étapes :

- DÉVELOPPEMENT — Les fonctions de cette étape peuvent être modifiées, testées et mises à jour. Utilisez cette étape pour écrire et déboguer le code de votre fonction.
- LIVE — Les fonctions de cette étape sont en lecture seule et gèrent le trafic de production. Vous ne pouvez pas modifier les fonctions directement dans la scène LIVE.

Lorsque vous créez une nouvelle fonction de connexion, elle démarre au stade de DÉVELOPPEMENT. Après le test et la validation, vous publiez la fonction pour la déplacer vers l'étape LIVE.

Flux de travail du développement

Suivez ce flux de travail pour développer et déployer Connection Functions :

1. Créer — Créez une nouvelle fonction de connexion au stade de DÉVELOPPEMENT avec votre code et votre configuration initiaux.
2. Test : utilisez la fonctionnalité de test pour valider votre fonction à l'aide d'exemples d'événements de connexion avant le déploiement.
3. Mettre à jour : modifiez le code de fonction et la configuration selon les besoins en fonction des résultats des tests.
4. Publier : lorsque vous êtes prête pour la production, publiez la fonction pour la faire passer du stade DEVELOPMENT au stade LIVE.
5. Associer : associez la fonction publiée à votre TLS-enabled distribution m pour gérer les connexions en direct.

Pour apporter des modifications à une fonction LIVE, vous devez mettre à jour la version DEVELOPMENT et la publier à nouveau. Cela crée une nouvelle version dans la scène LIVE.

Différences par rapport aux autres types de fonctions

Les fonctions de connexion diffèrent des fonctions de demande et de réponse du spectateur de plusieurs manières importantes :

- Les fonctions de connexion s'exécutent après l'établissement de la liaison mTLS, avant tout traitement HTTP
- Les fonctions de connexion ont accès aux informations du certificat TLS au lieu des données HTTP request/response
- Les fonctions de connexion peuvent uniquement autoriser ou refuser la connexion, pas modifier les données HTTP
- Les fonctions de connexion ne sont invoquées que pour les nouvelles connexions TLS, pas pour la réutilisation des connexions
- La reprise de session TLS n'est pas prise en charge avec mTLS pour garantir que la validation du certificat a lieu à chaque connexion

- Les fonctions de connexion s'exécutent en plus des fonctions standard de demande et de réponse du spectateur
- Vous associez les fonctions de connexion au niveau de la distribution plutôt qu'au niveau du comportement du cache.
- Les fonctions de connexion ne prennent en charge que le JavaScript runtime 2.0.

Configuration et limites

CloudFront Les fonctions de connexion ont des exigences de configuration et des limites de service spécifiques en raison de leur rôle spécialisé dans la validation des connexions TLS et des exigences de performance de l'informatique de pointe.

Rubriques

- Exigences relatives au code de fonction
- Service Limits
- Options de filtrage des fonctions

Exigences relatives au code de fonction

Les fonctions de connexion nécessitent un JavaScript code qui traite les événements de connexion TLS. Le code de fonction doit :

- Être écrit en JavaScript
- Traitez les événements de connexion et prenez allow/deny des décisions
- Exécution complète dans les délais
- Gérer la logique de validation des certificats et des connexions

Service Limits

Les fonctions de connexion sont soumises aux limites suivantes :

- Taille de la fonction — La taille du code de fonction et de la configuration est limitée
- Temps d'exécution : les fonctions ont des limites de temps d'exécution strictes pour le traitement des connexions TLS

- Limites d'association : chaque distribution ne peut avoir qu'une seule fonction de connexion associée
- Restrictions d'étape — Seules les fonctions d'étape LIVE peuvent être associées à des distributions

Options de filtrage des fonctions

Lorsque vous répertoriez les fonctions de connexion, vous pouvez utiliser les filtres suivants :

- Filtre d'étape — Filtrer par stade de développement ou stade en direct
- Filtre d'association : filtrez par identifiant de distribution ou par association d'identifiants de magasin clé-valeur

Ces filtres vous aident à organiser et à gérer les fonctions de connexion dans différents environnements et cas d'utilisation.

Création de fonctions de CloudFront connexion pour une validation mutuelle du protocole TLS (afficheur)

Vous créez une fonction de CloudFront connexion en deux étapes :

1. Créez le code de fonction sous la forme JavaScript. Vous pouvez utiliser l'exemple par défaut de la CloudFront console ou écrire le vôtre. Pour plus d'informations, consultez les rubriques suivantes :
   - Écrire le code CloudFront de la fonction de connexion pour la validation mTLS
   - CloudFront Structure des événements et format de réponse de la fonction de connexion
   - Exemples de code de fonction de connexion
2. CloudFront Utilisez-le pour créer la fonction de connexion et inclure votre code. Le code existe à l'intérieur de la fonction (et non en tant que référence).

Rubriques

- CloudFront console
- AWS CLI

CloudFront console

Pour créer une fonction de connexion

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Créer une fonction.
3. Entrez un nom de fonction unique dans le Compte AWS, choisissez Fonction de connexion comme type de fonction, puis choisissez Continuer.
4. La page de détails de la nouvelle fonction de connexion s'affiche.

   > **Note**
   >
   > Les fonctions de connexion ne prennent en charge que le JavaScript runtime 2.0. Pour utiliser l' KeyValueStore intégration de la fonction de CloudFront connexion dans la fonction, vous devez utiliser cette version d'exécution.

5. Dans la section Code de fonction, choisissez l'onglet Créer et entrez votre code de fonction de connexion. L'exemple de code inclus dans l'onglet Générer illustre la syntaxe de base du code de la fonction de connexion.
6. Cliquez sur Enregistrer les modifications.
7. Si le code de la fonction de connexion est utilisé KeyValueStore pour la vérification de la révocation du certificat ou la validation de l'appareil, vous devez associer un KeyValueStore.

   Vous pouvez l'associer KeyValueStore lorsque vous créez la fonction pour la première fois. Vous pouvez également l'associer ultérieurement, en associant des fonctions de connexion.

   Pour associer un KeyValueStore now, procédez comme suit :

   - Accédez à la KeyValueStore section Associer et choisissez Associer existant KeyValueStore.
   - Sélectionnez celui KeyValueStore qui contient les données de certificat pour votre fonction de connexion, puis choisissez Associer KeyValueStore.

   CloudFront associe immédiatement le magasin à la fonction. Vous n’avez pas besoin d’enregistrer la fonction.

AWS CLI

Si vous utilisez le AWS CLI, vous créez généralement d'abord le code de la fonction de connexion dans un fichier, puis créez la fonction avec le AWS CLI.

Pour créer une fonction de connexion

1. Créez le code de la fonction de connexion dans un fichier et stockez-le dans un répertoire auquel votre ordinateur peut se connecter.
2. Exécutez la commande, comme illustré dans l'exemple. Cet exemple utilise la notation `fileb://` pour transmettre le fichier. Il inclut également des sauts de ligne pour rendre la commande plus lisible.

```
aws cloudfront create-connection-function \
    --name CertificateValidator \
    --connection-function-config '{
        "Comment":"Device certificate validation",
        "Runtime":"cloudfront-js-2.0",
        "KeyValueStoreAssociations":{
            "Quantity":1,
            "Items":[{
                "KeyValueStoreARN":"arn:aws:cloudfront::111122223333:key-value-
store/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }]
        }
    }' \
    --connection-function-code fileb://certificate-validator.js
```

> **Note**
>
> - Runtime : les fonctions de connexion ne prennent en charge que le JavaScript runtime 2.0 (cloudfront-js-2.0).
> - KeyValueStoreAssociations— Si votre fonction de connexion l'utilise KeyValueStore pour la validation du certificat, vous pouvez l'associer KeyValueStore lorsque vous créez la fonction pour la première fois. Vous pouvez également l'associer ultérieurement, en utilisant la fonction update-connection-function. La quantité est toujours égale à 1 car chaque fonction de connexion ne peut être KeyValueStore associée qu'à une seule fonction.

3. Lorsque la commande s’exécute correctement, vous obtenez une sortie similaire à ce qui suit.

```
ETag: ETVABCEXAMPLE
ConnectionFunctionSummary:
  ConnectionFunctionConfig:
    Comment: Device certificate validation
    Runtime: cloudfront-js-2.0
    KeyValueStoreAssociations:
      Quantity: 1
      Items:
        - KeyValueStoreARN: arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
  ConnectionFunctionMetadata:
    CreatedTime: '2024-09-04T16:32:54.292000+00:00'
    ConnectionFunctionARN: arn:aws:cloudfront::111122223333:connection-function/
CertificateValidator
    LastModifiedTime: '2024-09-04T16:32:54.292000+00:00'
    Stage: DEVELOPMENT
  Name: CertificateValidator
  Status: UNPUBLISHED
Location: https://cloudfront.amazonaws.com/2020-05-31/connection-function/
arn:aws:cloudfront:::connection-function/CertificateValidator
```

La plupart des informations proviennent de la demande. D'autres informations sont ajoutées par CloudFront.

> **Note**
>
> - ETag — Cette valeur change chaque fois que vous modifiez la fonction de connexion. Vous avez besoin de cette valeur pour mettre à jour ou publier la fonction.
> - Étape — Les nouvelles fonctions de connexion démarrent au stade de DÉVELOPPEMENT. Vous devez publier la fonction pour la déplacer vers la scène LIVE avant de l'associer à une distribution.
> - État : le statut de la fonction est NON PUBLIÉ jusqu'à ce que vous la publiiez sur la scène LIVE.

Écrire le code de la fonction de CloudFront connexion pour la validation mutuelle du protocole TLS (afficheur)

CloudFront Les fonctions de connexion vous permettent d'écrire des JavaScript fonctions légères pour la validation des certificats mTLS et une logique d'authentification personnalisée. Le code de votre fonction de connexion peut valider les certificats clients, implémenter des règles d'authentification spécifiques à l'appareil, gérer des scénarios de révocation de certificats et prendre des allow/deny décisions concernant les connexions TLS sur des sites périphériques du monde entier. CloudFront

Les fonctions de connexion constituent un moyen puissant d'étendre la validation CloudFront intégrée des certificats à votre propre logique métier. Contrairement aux fonctions de demande et de réponse du visualiseur qui traitent les données HTTP, les fonctions de connexion fonctionnent au niveau de la couche TLS et ont accès aux informations de certificat, aux adresses IP des clients et aux détails de connexion TLS. Ils sont donc idéaux pour mettre en œuvre des modèles de sécurité zéro confiance, des systèmes d'authentification des appareils et des politiques de validation de certificats personnalisées qui vont au-delà de la validation PKI standard.

Le code de votre fonction de connexion s'exécute dans un environnement isolé et sécurisé avec des temps de démarrage inférieurs à la milliseconde et peut évoluer pour gérer des millions de connexions par seconde. Le runtime est optimisé pour les charges de travail de validation des certificats et fournit une intégration intégrée aux opérations de recherche de données en temps réel, permettant des scénarios d'authentification sophistiqués tels que la vérification de la liste de révocation des certificats et la validation de la liste d'autorisation des appareils. CloudFront KeyValueStore

Pour vous aider à écrire un code de fonction de connexion efficace, consultez les rubriques suivantes. Pour des exemples de code complets et des didacticiels étape par étape, consultez les sections didacticielles de ce guide et explorez les exemples de fonctions de connexion disponibles dans la CloudFront console.

Rubriques

- CloudFront Cas d'utilisation et objectifs de la fonction de connexion
- CloudFront Structure des événements et format de réponse de la fonction de connexion
- CloudFront Fonctionnalités d' JavaScript exécution de Connection Functions
- CloudFront Méthodes d'assistance et API de la fonction de connexion
- CloudFront KeyValueStore Intégration de la fonction de connexion

- Utilisez async et attendez
- Exemples de code de fonction de connexion

CloudFront Cas d'utilisation et objectifs de la fonction de connexion

Avant d'écrire votre fonction de CloudFront connexion, déterminez soigneusement le type de logique de validation de certificat ou d'authentification que vous devez implémenter. Les fonctions de connexion sont conçues pour des cas d'utilisation spécifiques qui nécessitent une validation personnalisée allant au-delà de la vérification standard des certificats PKI. Comprendre votre cas d'utilisation vous permet de concevoir un code efficace qui répond à vos exigences de sécurité tout en maintenant des performances optimales.

Les cas d'utilisation courants de la fonction de connexion incluent :

- Gestion des révocations de certificats : mettez en œuvre des politiques personnalisées pour gérer les certificats révoqués, notamment des délais de grâce pour la rotation des certificats, des exceptions réseau fiables pour les périphériques internes ou des scénarios d'accès d'urgence dans lesquels les certificats révoqués peuvent nécessiter un accès temporaire.
- Support mTLS en option : gérez à la fois les connexions mTLS et non MTLS avec différentes politiques d'authentification, ce qui vous permet de renforcer la sécurité des clients qui prennent en charge les certificats tout en maintenant la compatibilité avec les clients existants.
- IP-based authentification : associez la validation des certificats à la vérification des adresses IP des clients pour renforcer la sécurité, par exemple en restreignant l'accès depuis des régions géographiques spécifiques, des réseaux d'entreprise ou des plages d'adresses IP malveillantes connues.
- Multi-tenant validation des certificats : implémentez des règles de validation spécifiques au locataire dans lesquelles différentes autorités de certification ou différents critères de validation s'appliquent en fonction des attributs de l'émetteur du certificat client ou du sujet.
- Time-based contrôle d'accès : appliquez des restrictions temporelles selon lesquelles les certificats ne sont valides que pendant des heures, des périodes de maintenance ou des périodes ouvrables spécifiques, même si le certificat lui-même n'a pas expiré.

Les fonctions de connexion s' CloudFront exécutent après avoir effectué la validation standard des certificats (vérification de la chaîne de confiance, contrôles d'expiration et validation de signature) mais avant l'établissement de la connexion TLS. Ce calendrier vous permet d'ajouter des critères de validation personnalisés tout en bénéficiant de la validation des certificats CloudFront intégrée. Votre

fonction reçoit les résultats de la validation standard et peut prendre des décisions éclairées quant à l'autorisation ou au refus de la connexion sur la base de critères standard et personnalisés.

Lors de la conception de votre fonction de connexion, tenez compte des implications de votre logique de validation en termes de performances. Les fonctions ayant une limite d'exécution de 5 millisecondes, les opérations complexes doivent être optimisées en termes de vitesse. Utilisez-le KeyValueStore pour des recherches de données rapides plutôt que pour des calculs complexes, et structurez votre logique de validation pour qu'elle échoue rapidement en cas de certificats non valides.

CloudFront Structure des événements et format de réponse de la fonction de connexion

CloudFront Les fonctions de connexion reçoivent une structure d'événements différente de celle des fonctions de demande et de réponse des spectateurs. Au lieu des request/response données HTTP, les fonctions de connexion reçoivent des informations de certificat et de connexion que vous pouvez utiliser pour prendre des décisions d'authentification.

Rubriques

- Structure des événements pour Connection Functions
- Format de réponse des fonctions de connexion

Structure des événements pour Connection Functions

Les fonctions de connexion reçoivent un objet d'événement contenant des informations de certificat et de connexion. La structure des événements de la fonction est illustrée ci-dessous :

```
{
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "serialNumber": "string",
        "issuer": "string",
        "subject": "string",
        "validity": {
          "notBefore": "string",
          "notAfter": "string"
        },
        "sha256Fingerprint": "string",
        "ocspEndpoint": "string",
```

```
        "san": "string",
        "spki": "string",
        "sanHex": "string"
      },
      "intermediates": [
        {
          "serialNumber": "string",
          "issuer": "string",
          "subject": "string",
          "validity": {
            "notBefore": "string",
            "notAfter": "string"
          },
          "sha256Fingerprint": "string",
          "ocspEndpoint": "string",
          "san": "string",
          "spki": "string",
          "sanHex": "string"
        }
      ]
    }
  },
  "clientIp": "string",
  "endpoint": "string",
  "distributionId": "string",
  "connectionId": "string"
}
```

Vous trouverez ci-dessous un exemple de structure d'objet d'événement :

```
{
  "clientCertificate": {
    "certificates": {
      "leaf": {
        "serialNumber": "00:9e:2a:af:16:56:e5:47:25:7d:2e:38:c3:f9:9d:57:fa",
        "issuer": "C=US, O=Ram, OU=Edge, ST=WA, CN=mTLS-CA, L=Snoqualmie",
        "subject": "C=US, O=Ram, OU=Edge, ST=WA, CN=mTLS-CA, L=Snoqualmie",
        "validity": {
          "notBefore": "2025-09-10T23:43:10Z",
          "notAfter": "2055-09-11T00:43:02Z"
        },
        "sha256Fingerprint": "_w6bJ7aOAlGOj7NUhJxTfsfee-ONg_xop3_PTgTJpqs=",
        "ocspEndpoint": "http://ocsp.example.com",
```

```
        "san": "DNS:api.example.com,DNS:www.example.com,URI:urn:example:client:123,IP
 Address:192.168.1.100,email:alejandro_rosalez@example.com",
        "spki":
 "30820122300d06092a864886f70d01010105000382010f003082010a0282010100b8efe87db798500320936...",
        "sanHex":
 "3058820f6170692e6578616d706c652e636f6d820f7777772e6578616d706c652e636f6d8619..."
      },
      "intermediates": [
        {
          "serialNumber": "00:d4:04:a5:fd:cb:20:37:54",
          "issuer": "C=US, O=Example Corp, CN=Example Root CA",
          "subject": "C=US, O=Example Corp, CN=Example Intermediate CA",
          "validity": {
            "notBefore": "2024-01-01T00:00:00Z",
            "notAfter": "2034-01-01T23:59:59Z"
          },
          "sha256Fingerprint": "3a8c6b...",
          "ocspEndpoint": "http://ocsp.example.com/intermediate",
          "san": "DNS:ca.example.com,URI:urn:ca:intermediate:001",
          "spki":
 "30820122300d06092a864886f70d01010105000382010f003082010a0282010100b389dd513b0f1f14cac1...",
          "sanHex": "302b820e63612e6578616d706c652e636f6d..."
        }
      ]
    }
  },
  "clientIp": "192.0.2.1",
  "endpoint": "d3lch071jze0cb.cloudfront.net",
  "distributionId": "E1NXS4MQZH501R",
  "connectionId": "NpvTe1925xfj24a67sPQr7ae42BIq03FGhJJKfrQYWZcWZFp96SIIg=="
}
```

Format de réponse des fonctions de connexion

Votre fonction de connexion doit renvoyer un objet de réponse indiquant s'il faut autoriser ou refuser la connexion. Utilisez les méthodes d'assistance pour prendre des décisions de connexion :

```
function connectionHandler(connection) {
    // Helper methods to allow or deny connections
    if (/* some logic to determine if function should allow connection */) {
        connection.allow();
    } else {
        connection.deny();
```

```
    }
}
```

Contrairement aux fonctions de demande et de réponse du visualiseur, les fonctions de connexion ne peuvent pas modifier les requêtes ou les réponses HTTP. Ils peuvent uniquement autoriser ou refuser la connexion TLS.

CloudFront Fonctionnalités d' JavaScript exécution de Connection Functions

CloudFront Connection Functions utilise le JavaScript runtime CloudFront Functions 2.0, qui fournit un environnement sécurisé et performant spécialement optimisé pour les charges de travail de validation des certificats. Le runtime est conçu pour démarrer en moins de millisecondes et gérer des millions d'exécutions simultanées sur le réseau périphérique CloudFront mondial.

L'environnement d'exécution inclut une prise en charge JavaScript linguistique complète :

- Prise en charge d'ECMAScript 2020 (ES11) : JavaScript fonctionnalités modernes, notamment le chaînage optionnel (?.) et fusion nulle (? ?)
- Built-in objets : JavaScript objets standard tels que Object, Array, JSON, Math et Date
- Journalisation de la console : utilisez console.log () pour déboguer et surveiller les décisions de validation des certificats. Les journaux sont disponibles en temps réel pendant les tests et peuvent aider à résoudre les problèmes liés à la logique de validation en cours de développement
- KeyValueStore intégration : accès natif CloudFront KeyValueStore pour des opérations de recherche de données ultrarapides, permettant la vérification de la révocation des certificats en temps réel, la validation de la liste d'autorisation des appareils et la récupération de la configuration spécifique au locataire

Les fonctions de connexion sont optimisées pour des performances élevées pour les scénarios de validation de certificats. Le moteur d'exécution gère automatiquement la gestion de la mémoire, le ramassage des déchets et le nettoyage des ressources afin de garantir des performances constantes sur des millions de connexions simultanées. Toutes les opérations sont conçues pour être déterministes et rapides, les recherches se terminant généralement KeyValueStore en quelques microsecondes.

L'environnement d'exécution est complètement isolé entre les exécutions de fonctions, ce qui garantit qu'aucune donnée ne fuit entre les différentes connexions client. Chaque exécution de fonction commence par un état propre et n'a aucun accès aux résultats d'exécution précédents ni aux données client provenant d'autres connexions.

CloudFront Méthodes d'assistance et API de la fonction de connexion

CloudFront Les fonctions de connexion fournissent des méthodes d'assistance spécialisées conçues pour simplifier les décisions relatives à la validation des certificats et améliorer l'observabilité. Ces méthodes sont optimisées pour le flux de validation des connexions et s'intègrent parfaitement aux systèmes d'enregistrement et de surveillance des CloudFront connexions.

- connection.allow () — Autorise la connexion TLS à se poursuivre. Cette méthode indique CloudFront de terminer l'établissement de la liaison TLS et de permettre au client d'établir la connexion. Utilisez-le lorsque la validation du certificat est réussie et que toute logique d'authentification personnalisée est satisfaite
- connection.deny () — Refuse la connexion TLS et met fin à la poignée de main. Cette méthode ferme immédiatement la connexion et empêche tout trafic HTTP de circuler. Le client recevra une erreur de connexion TLS. Utilisez-le pour les certificats non valides, les échecs d'authentification ou les violations des politiques
- connection.log CustomData () — Ajoutez des données personnalisées aux journaux de connexion (jusqu'à 800 octets de UTF-8 texte). Cette méthode vous permet d'inclure les résultats de validation, les détails du certificat ou la justification de la décision dans les journaux de CloudFront connexion à des fins de surveillance de la sécurité, d'audit de conformité et de dépannage

Ces méthodes fournissent une interface déclarative claire pour prendre des décisions de connexion et enregistrer les informations pertinentes pour la surveillance et le débogage. Le allow/deny modèle garantit que l'intention de votre fonction est claire et CloudFront permet d'optimiser la gestion des connexions en fonction de votre décision. Les données de journalisation personnalisées sont immédiatement disponibles dans les journaux de CloudFront connexion et peuvent être utilisées avec des outils d'analyse des journaux pour la surveillance de la sécurité et des informations opérationnelles.

Appelez toujours connection.allow () ou connection.deny () avant que votre fonction ne soit terminée. Si aucune méthode n'est appelée, la connexion CloudFront sera refusée par défaut par mesure de sécurité.

CloudFront KeyValueStore Intégration de la fonction de connexion

CloudFront Les fonctions de connexion peuvent être utilisées CloudFront KeyValueStore pour effectuer des recherches de données ultrarapides pour des scénarios de validation de certificats. KeyValueStore est particulièrement puissant pour les fonctions de connexion, car il fournit un accès

global aux données, éventuellement cohérent, avec des temps de recherche de l'ordre de l'ordre de la microseconde sur tous les CloudFront emplacements périphériques. Il est donc idéal pour gérer les listes de révocation de certificats, les listes d'appareils autorisés, les configurations des locataires et d'autres données de validation qui doivent être accessibles lors des handshakes TLS.

KeyValueStore l'intégration est conçue spécifiquement pour les flux de validation de connexion performants :

- kvs Handle.exists (key) — Vérifie si une clé existe dans le KeyValueStore sans récupérer la valeur. Il s'agit de la méthode la plus efficace pour les scénarios de validation binaire tels que la vérification de la révocation des certificats, dans le cadre de laquelle il vous suffit de savoir si le numéro de série d'un certificat figure dans une liste de révocation.
- kvs Handle.get (key) — Récupère une valeur à partir de KeyValueStore pour des scénarios de validation plus complexes. Utilisez-le lorsque vous devez accéder à des données de configuration, à des règles de validation ou à des métadonnées associées à un certificat ou à un identifiant d'appareil

KeyValueStore les opérations sont asynchrones et doivent être utilisées avec async/await la syntaxe. KeyValueStore Il a une limite de taille totale de 10 Mo et prend en charge jusqu'à 10 millions de paires clé-valeur. KeyValueStore les données sont finalement cohérentes sur tous les emplacements périphériques, les mises à jour se propageant généralement en quelques secondes.

Pour des performances optimales, structurez vos KeyValueStore clés de manière à minimiser les opérations de recherche. Utilisez les numéros de série des certificats comme clés pour une simple vérification de révocation, ou créez des clés composites combinant le hachage de l'émetteur et le numéro de série pour les environnements multi-CA. Tenez compte des compromis entre complexité et KeyValueStore capacité clés lors de la conception de votre structure de données.

Utilisez async et attendez

Les fonctions de connexion prennent en charge les opérations asynchrones à l'aide de async/await la syntaxe, ce qui est essentiel lorsque vous travaillez avec KeyValueStore des opérations ou d'autres tâches asynchrones. Le async/await modèle garantit que votre fonction attend la fin des KeyValueStore recherches avant de prendre des décisions de connexion, tout en conservant les caractéristiques de haute performance requises pour le traitement des handshake TLS.

async/await L'utilisation correcte des fonctions de connexion est essentielle car les KeyValueStore opérations, bien que très rapides, restent des opérations réseau qui nécessitent une coordination

au sein de l'infrastructure CloudFront distribuée. Le runtime gère automatiquement la résolution des promesses et s'assure que votre fonction se termine dans la limite d'exécution de 5 millisecondes.

Example: Fonction de connexion asynchrone avec KeyValueStore

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Async operation to check KeyValueStore for certificate revocation
    const isRevoked = await
 kvsHandle.exists(connection.clientCertificate.certificates.leaf.serialNumber);

    if (isRevoked) {
        // Log the revocation decision with certificate details
        connection.logCustomData(`REVOKED_CERT:
${connection.clientCertificate.certificates.leaf.serialNumber}:
${connection.clientCertificate.certificates.leaf.issuer}`);
        console.log(`Denying connection for revoked certificate:
 ${connection.clientCertificate.certificates.leaf.serialNumber}`);
        return connection.deny();
    }

    // Log successful validation for monitoring
    connection.logCustomData(`VALID_CERT:
${connection.clientCertificate.certificates.leaf.serialNumber}`);
    console.log(`Allowing connection for valid certificate:
 ${connection.clientCertificate.certificates.leaf.serialNumber}`);
    return connection.allow();
}
```

À toujours utiliser async/await lors de l'appel KeyValueStore de méthodes ou d'autres opérations asynchrones. L'environnement d'exécution de la fonction de connexion gère automatiquement la résolution des promesses et garantit un flux d'exécution correct dans les strictes contraintes temporelles du traitement TLS handshake. Évitez d'utiliser .then () ou des modèles de rappel, car cela async/await permet une gestion plus claire des erreurs et de meilleures performances dans l'environnement Connection Function.

Lorsque vous concevez des fonctions de connexion asynchrones, structurez votre code de manière à minimiser le nombre d' KeyValueStore opérations et exécutez-les le plus tôt possible dans votre logique de validation. Cela garantit des performances optimales et réduit le risque de problèmes

de temporisation pendant les périodes de forte affluence. Envisagez de regrouper les contrôles de validation liés aux lots et d'utiliser la KeyValueStore méthode la plus efficace (exists () contre get ()) pour votre cas d'utilisation.

Exemples de code de fonction de connexion

Les exemples suivants présentent des modèles de fonctions de connexion courants pour différents scénarios de validation. Utilisez ces exemples comme point de départ pour vos propres implémentations de fonctions de connexion.

Example: Validation du certificat de l'appareil

Cet exemple valide les numéros de série des appareils et les champs d'objet de certificat pour les appareils IoT, les consoles de jeu et d'autres scénarios d'authentification client :

```
async function connectionHandler(connection) {
    // Custom validation: check device serial number format
    const serialNumber = connection.clientCertificate.certificates.leaf.serialNumber;
    if (!serialNumber.startsWith("DEV")) {
        connection.logCustomData(`INVALID_SERIAL:${serialNumber}`);
        return connection.deny();
    }

    // Validate certificate subject contains required organizational unit
    const subject = connection.clientCertificate.certificates.leaf.subject;
    if (!subject.includes("OU=AuthorizedDevices")) {
        connection.logCustomData(`INVALID_OU:${subject}`);
        return connection.deny();
    }

    // Allow connection for valid devices
    connection.logCustomData(`VALID_DEVICE:${serialNumber}`);
    return connection.allow();
}
```

Cette fonction effectue plusieurs contrôles de validation au-delà de la validation standard des certificats, notamment le format du numéro de série de l'appareil et la vérification des unités organisationnelles.

Example: mTL en option avec authentification mixte

Cet exemple gère à la fois les connexions mTLS et non MTLS avec des politiques d'authentification différentes :

```
async function connectionHandler(connection) {
    if (connection.clientCertificate) {
        // mTLS connection - enhanced validation for certificate holders
        const subject = connection.clientCertificate.certificates.leaf.subject;
        connection.logCustomData(`MTLS_SUCCESS:${subject}:${connection.clientIp}`);
        console.log(`mTLS connection from: ${subject}`);
        return connection.allow();
    } else {
        // Non-mTLS connection - apply IP-based restrictions
        const clientIp = connection.clientIp;

        // Only allow non-mTLS from specific IP ranges
        if (clientIp.startsWith("203.0.113.") || clientIp.startsWith("198.51.100.")) {
            connection.logCustomData(`NON_MTLS_ALLOWED:${clientIp}`);
            console.log(`Non-mTLS connection allowed from: ${clientIp}`);
            return connection.allow();
        }

        connection.logCustomData(`NON_MTLS_DENIED:${clientIp}`);
        return connection.deny();
    }
}
```

Cette fonction fournit une sécurité accrue aux clients détenteurs de certificats tout en maintenant la compatibilité avec les anciens clients issus de plages IP fiables.

Testez les fonctions de CloudFront connexion avant le déploiement

Vous pouvez tester les fonctions de CloudFront connexion au stade de DÉVELOPPEMENT à l'aide de l'opération TestConnectionFunction API. Grâce aux tests, vous pouvez valider la logique de votre fonction à l'aide d'exemples d'événements de connexion avant de publier sur la scène LIVE.

Rubriques

- Processus de test
- Résultats des tests
- Objet de test de connexion

Processus de test

Pour tester une fonction de connexion :

1. Création d'une fonction de connexion en phase de développement
2. Préparez un objet de connexion de test qui représente l'événement de connexion TLS
3. Utilisez l'opération TestConnectionFunction API pour exécuter votre fonction avec les données de test
4. Passez en revue les résultats des tests, y compris les résultats des fonctions, les journaux d'exécution et les éventuels messages d'erreur
5. Mettez à jour le code de votre fonction si nécessaire et répétez le processus de test

Résultats des tests

Lorsque vous testez une fonction de connexion, les résultats incluent :

- Résumé des fonctions : métadonnées relatives à la fonction qui a été testée
- Utilisation du calcul : mesures de performance indiquant l'utilisation des ressources
- Journaux d'exécution : sortie de console de votre fonction, y compris toutes les instructions de journalisation
- Sortie de fonction — Le résultat renvoyé par votre fonction
- Messages d'erreur : toutes les erreurs d'exécution ou les exceptions survenues pendant l'exécution

Objet de test de connexion

L'objet de test de connexion est un blob binaire (jusqu'à 40 Ko) qui représente l'événement de connexion TLS que votre fonction va traiter. Cet objet contient le certificat et les informations de connexion que votre fonction utilise pour prendre des décisions d'authentification.

> **Note**
>
> La structure et le format spécifiques de l'objet de test de connexion sont définis par le moteur d'exécution CloudFront Connection Functions. Consultez la documentation CloudFront des fonctions ou contactez-nous AWS Support pour plus de détails sur la création d'objets de test adaptés à votre cas d'utilisation.

Après avoir créé votre fonction de connexion, vous pouvez :

- Testez la fonction : utilisez la fonctionnalité de test de la console ou de l'interface de ligne de commande pour valider votre fonction à l'aide d'exemples d'événements de connexion. Pour plus d'informations, consultez la section Test des fonctions de connexion.
- Mettre à jour la fonction — Modifiez le code et la configuration de la fonction selon les besoins. Les fonctions de connexion en phase de DÉVELOPPEMENT peuvent être mises à jour à tout moment.
- Publier la fonction — Une fois prête pour la production, publiez la fonction pour la faire passer du stade DEVELOPMENT au stade LIVE. Pour plus d'informations, consultez la section Associer des fonctions de connexion.
- Associer à une distribution : associez la fonction publiée à une TLS-enabled distribution m pour gérer les connexions en direct. Pour plus d'informations, consultez la section Associer des fonctions de connexion.

Associer les fonctions de connexion aux distributions

Après avoir publié une fonction de connexion sur la scène LIVE, vous devez l'associer à une TLS-enabled distribution m pour gérer les connexions en direct. Les fonctions de connexion sont associées au niveau de la distribution, contrairement aux fonctions de demande et de réponse des spectateurs qui sont associées aux comportements du cache.

Rubriques

- Exigences de l'association
- Organisation des fonctions à l'aide de filtres
- Considérations relatives au déploiement

Exigences de l'association

Pour associer une fonction de connexion à une distribution :

- La fonction doit être en phase LIVE
- La distribution doit avoir mTLS activé
- La distribution doit disposer d'un magasin de confiance valide configuré
- Vous ne pouvez associer qu'une seule fonction de connexion par distribution

Organisation des fonctions à l'aide de filtres

CloudFront fournit des fonctionnalités de filtrage pour vous aider à organiser et à gérer les fonctions de connexion :

- Filtre d'identifiant de distribution — Trouvez des fonctions associées à des distributions spécifiques
- Key-value filtre de stockage — Trouvez des fonctions qui utilisent des magasins de valeurs clés spécifiques pour la recherche de données
- Filtre de scène — Répertoriez les fonctions dans la phase DEVELOPMENT ou LIVE

Utilisez ces filtres lorsque vous gérez plusieurs fonctions de connexion dans différentes distributions ou environnements de développement.

Considérations relatives au déploiement

Tenez compte des facteurs suivants lors du déploiement de Connection Functions :

- Déploiement mondial : les fonctions de connexion sont déployées CloudFront sur tous les sites périphériques du monde entier, ce qui peut prendre plusieurs minutes
- Gestion des versions — Chaque version publiée crée une nouvelle fonction LIVE qui remplace la version précédente
- Stratégie de restauration : planifiez la restauration en conservant les versions fonctionnelles précédentes du code de votre fonction
- Tests en production — Envisagez d'utiliser des distributions distinctes pour les environnements de test et de production

Implémentez la révocation des certificats pour le TLS mutuel (visualiseur) avec CloudFront Functions et KeyValueStore

Vous pouvez utiliser CloudFront Connection Functions avec KeyValueStore pour implémenter la vérification de révocation des certificats. Vous pouvez ainsi conserver une liste des numéros de série des certificats révoqués et comparer les certificats clients à cette liste lors de la prise de contact TLS.

Pour implémenter la révocation des certificats, vous avez besoin des composants suivants :

- Une distribution configurée avec Viewer mTLS
- A KeyValueStore contenant les numéros de série des certificats révoqués

- Une fonction de connexion qui interroge le KeyValueStore pour vérifier l'état du certificat

Lorsqu'un client se connecte, CloudFront valide le certificat par rapport au Trust Store, puis exécute votre fonction de connexion. Votre fonction vérifie le numéro de série du certificat par rapport au numéro de série KeyValueStore et autorise ou refuse la connexion.

Rubriques

- Étape 1 : créer un formulaire KeyValueStore pour les certificats révoqués
- Étape 2 : Création de la fonction de connexion de révocation
- Étape 3 : Testez votre fonction de révocation
- Étape 4 : Associez la fonction à votre distribution
- Scénarios de révocation avancés

Étape 1 : créer un formulaire KeyValueStore pour les certificats révoqués

Créez un KeyValueStore pour stocker les numéros de série des certificats révoqués que votre fonction de connexion peut vérifier lors des connexions mTLS.

Commencez par préparer les numéros de série de vos certificats révoqués au format JSON :

```
{
  "data": [
    {
      "key": "ABC123DEF456",
      "value": ""
    },
    {
      "key": "789XYZ012GHI",
      "value": ""
    }
  ]
}
```

Téléchargez ce fichier JSON dans un compartiment S3, puis créez KeyValueStore :

```
aws s3 cp revoked-serials.json s3://your-bucket-name/revoked-serials.json
aws cloudfront create-key-value-store \
  --name revoked-serials-kvs \
```

```
  --import-source '{
    "SourceType": "S3",
    "SourceARN": "arn:aws:s3:::your-bucket-name/revoked-serials.json"
  }'
```

Attendez la fin KeyValueStore du provisionnement. Vérifiez le statut avec :

```
aws cloudfront get-key-value-store --name "revoked-serials-kvs"
```

Étape 2 : Création de la fonction de connexion de révocation

Créez une fonction de connexion qui vérifie les numéros de série des certificats par rapport KeyValueStore à pour déterminer si les certificats sont révoqués.

Créez une fonction de connexion qui vérifie les numéros de série des certificats par rapport aux éléments KeyValueStore suivants :

```
aws cloudfront create-connection-function \
  --name "revocation-control" \
  --connection-function-config file://connection-function-config.json \
  --connection-function-code file://connection-function-code.txt
```

Le fichier de configuration spécifie l' KeyValueStore association :

```
{
  "Runtime": "cloudfront-js-2.0",
  "Comment": "A function that implements revocation control via KVS",
  "KeyValueStoreAssociations": {
    "Quantity": 1,
    "Items": [
      {
        "KeyValueStoreArn": "arn:aws:cloudfront::account-id:key-value-store/kvs-id"
      }
    ]
  }
}
```

Le code de la fonction de connexion vérifie s'il n'y a KeyValueStore pas de certificats révoqués :

```
import cf from 'cloudfront';
```

```
async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();

    // Get parsed client serial number from client certificate
    const clientSerialNumber = connection.clientCertInfo.serialNumber;

    // Check KVS to see if serial number exists as a key
    const serialNumberExistsInKvs = await kvsHandle.exists(clientSerialNumber);

    // Deny connection if serial number exists in KVS
    if (serialNumberExistsInKvs) {
        console.log("Connection denied - certificate revoked");
        return connection.deny();
    }

    // Allow connections that don't exist in kvs
    console.log("Connection allowed");
    return connection.allow();
}
```

Étape 3 : Testez votre fonction de révocation

Utilisez la CloudFront console pour tester votre fonction de connexion à l'aide d'exemples de certificats. Accédez à la fonction de connexion dans la console et utilisez l'onglet Test.

Test avec des exemples de certificats

1. Collez un exemple de certificat au format PEM dans l'interface de test
2. Spécifiez éventuellement une adresse IP client pour tester IP-based la logique
3. Choisissez la fonction de test pour voir les résultats d'exécution
4. Consultez les journaux d'exécution pour vérifier la logique de votre fonction

Testez avec des certificats valides et révoqués pour vous assurer que votre fonction gère correctement les deux scénarios. Les journaux d'exécution affichent la sortie du fichier console.log et toutes les erreurs survenues lors de l'exécution de la fonction.

Étape 4 : Associez la fonction à votre distribution

Après avoir publié votre fonction de connexion, associez-la à votre TLS-enabled distribution m pour activer la vérification de révocation des certificats.

Vous pouvez associer la fonction depuis la page des paramètres de distribution ou depuis le tableau des distributions associées à la fonction de connexion. Accédez à vos paramètres de distribution, accédez à la section Viewer Mutual Authentication (mTLS), sélectionnez votre fonction de connexion et enregistrez les modifications.

Scénarios de révocation avancés

Pour des exigences de révocation de certificats plus complexes, considérez les configurations supplémentaires suivantes :

Rubriques

- Convertir les listes de révocation de certificats (CRL) au format KeyValueStore
- Gérez plusieurs autorités de certification
- Ajouter des données personnalisées aux journaux de connexion
- Gérer les mises à jour de la CRL
- KeyValueStore Capacité du plan

Convertir les listes de révocation de certificats (CRL) au format KeyValueStore

Si vous possédez un fichier de liste de révocation de certificats (CRL), vous pouvez le convertir au format KeyValueStore JSON à l'aide d'OpenSSL et de jq :

Convertir CRL au KeyValueStore format

Extrayez les numéros de série du fichier CRL :

```
openssl crl -text -noout -in rfc5280_CRL.crl | \
  awk '/Serial Number:/ {print $3}' | \
  cut -d'=' -f2 | \
  sed 's/../&:/g;s/:$//' >> serialnumbers.txt
```

Convertissez les numéros de série au format KeyValueStore JSON :

```
jq -R -s 'split("\n") | map(select(length > 0)) | {data: map({"key": ., "value": ""})}'
 \
  serialnumbers.txt >> serialnumbers_kvs.json
```

Téléchargez le fichier formaté sur S3 et créez-le KeyValueStore comme décrit à l'étape 1.

Gérez plusieurs autorités de certification

Lorsque vous avez TrustStore plusieurs autorités de certification (CA), incluez les informations relatives à l'émetteur dans vos KeyValueStore clés afin d'éviter les conflits entre les certificats de différentes autorités de certification qui pourraient avoir le même numéro de série.

Pour les scénarios multi-CA, utilisez une combinaison du hachage SHA1 de l'émetteur et du numéro de série comme clé :

```
import cf from 'cloudfront';

async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();
    const clientCert = connection.clientCertInfo;

    // Create composite key with issuer hash and serial number
    const issuer = clientCert.issuer.replace(/[^a-zA-Z0-9]/g, '').substring(0, 20);
    const serialno = clientCert.serialNumber;
    const compositeKey = `${issuer}_${serialno}`;

    const cert_revoked = await kvsHandle.exists(compositeKey);

    if (cert_revoked) {
        console.log(`Blocking revoked cert: ${serialno} from issuer: ${issuer}`);
        connection.deny();
    } else {
        connection.allow();
    }
}
```

> **Note**
>
> L'utilisation de l'identifiant de l'émetteur et du numéro de série crée des clés plus longues, ce qui peut réduire le nombre total d'entrées que vous pouvez stocker dans le KeyValueStore.

Ajouter des données personnalisées aux journaux de connexion

Les fonctions de connexion peuvent ajouter des données personnalisées aux journaux de CloudFront connexion à l'aide de la CustomData méthode log. Vous pouvez ainsi inclure les résultats des

contrôles de révocation, les informations sur les certificats ou d'autres données pertinentes dans vos journaux.

```
async function connectionHandler(connection) {
    const kvsHandle = cf.kvs();
    const clientSerialNumber = connection.clientCertInfo.serialNumber;
    const serialNumberExistsInKvs = await kvsHandle.exists(clientSerialNumber);

    if (serialNumberExistsInKvs) {
        // Log revocation details to connection logs
        connection.logCustomData(`REVOKED:${clientSerialNumber}:DENIED`);
        console.log("Connection denied - certificate revoked");
        return connection.deny();
    }

    // Log successful validation
    connection.logCustomData(`VALID:${clientSerialNumber}:ALLOWED`);
    console.log("Connection allowed");
    return connection.allow();
}
```

Les données personnalisées sont limitées à 800 octets de UTF-8 texte valide. Si vous dépassez cette limite, CloudFront tronque les données à la limite valide UTF-8 la plus proche.

> **Note**
>
> L'enregistrement des données personnalisé ne fonctionne que lorsque les journaux de connexion sont activés pour votre distribution. Si les journaux de connexion ne sont pas configurés, la CustomData méthode de journalisation est inopérante.

Gérer les mises à jour de la CRL

Les autorités de certification peuvent émettre deux types de CRL :

- CRL complètes : contiennent une liste complète de tous les certificats révoqués
- CRL Delta : liste uniquement les certificats révoqués depuis la dernière CRL complète

Pour les mises à jour complètes de la CRL, créez-en une nouvelle KeyValueStore avec les données mises à jour et redirigez l'association de la fonction de connexion vers la nouvelle KeyValueStore.

Cette approche est plus simple que le calcul des différences et l'exécution de mises à jour incrémentielles.

Pour les mises à jour de la CRL delta, utilisez la commande update-keys pour ajouter de nouveaux certificats révoqués aux certificats existants : KeyValueStore

```
aws cloudfront update-key-value-store \
  --name "revoked-serials-kvs" \
  --if-match "current-etag" \
  --put file://delta-revoked-serials.json
```

KeyValueStore Capacité du plan

KeyValueStore a une taille limite de 5 Mo et prend en charge jusqu'à 10 millions de paires clé-valeur. Planifiez la capacité de votre liste de révocation en fonction du format de votre clé et de la taille des données :

- Numéro de série uniquement : stockage efficace pour un contrôle de révocation simple
- Identifiant de l'émetteur + numéro de série : clés plus longues pour les environnements multi-CA

Pour les listes de révocation volumineuses, envisagez de mettre en œuvre une approche à plusieurs niveaux dans laquelle vous les distinguerez KeyValueStores pour différentes catégories de certificats ou différentes périodes.

Personnalisation en périphérie avec Lambda@Edge

Lambda @Edge est une extension de. AWS Lambda Lambda @Edge est un service de calcul que vous pouvez utiliser pour exécuter des fonctions qui personnalisent le contenu diffusé par Amazon CloudFront . Vous pouvez créer des Node.js fonctions Python dans la console Lambda dans l'une d'entre elles Région AWS, dans l'est des États-Unis (Virginie du Nord).

Après avoir créé la fonction, vous pouvez ajouter des déclencheurs à l'aide de la console Lambda ou CloudFront de la console Lambda afin que les fonctions s'exécutent dans AWS des emplacements plus proches du visualiseur, sans provisionner ni gérer de serveurs. Vous pouvez éventuellement utiliser les opérations Lambda et CloudFront API pour configurer vos fonctions et vos déclencheurs par programmation.

Lambda@Edge s'adapte automatiquement, de quelques requêtes par jour jusqu'à des milliers de requêtes par seconde. Le traitement des demandes à AWS des emplacements plus proches de

l'utilisateur plutôt que sur les serveurs d'origine réduit considérablement le temps de latence et améliore l'expérience utilisateur.

> **Note**
>
> Lambda@Edge n’est pas pris en charge avec les demandes gRPC. Pour plus d’informations, consultez Utilisation de gRPC avec des distributions CloudFront.

Rubriques

- Fonctionnement de Lambda@Edge avec les demandes et les réponses
- Comment utiliser Lambda@Edge
- Mise en route des fonctions Lambda@Edge (console)
- Définition des autorisations et rôles IAM pour Lambda@Edge
- Écriture et création d’une fonction Lambda@Edge
- Ajout de déclencheurs pour une fonction Lambda@Edge
- Test et débogage des fonctions Lambda@Edge
- Suppression des fonctions et des réplicas Lambda@Edge
- Structure d'événement Lambda@Edge
- Utilisation des demandes et des réponses
- Exemples de fonctions Lambda@Edge

Fonctionnement de Lambda@Edge avec les demandes et les réponses

Lorsque vous associez une CloudFront distribution à une fonction Lambda @Edge, elle CloudFront intercepte les demandes et les réponses à CloudFront des emplacements périphériques. Vous pouvez exécuter des fonctions Lambda lorsque les CloudFront événements suivants se produisent :

- Quand CloudFront reçoit une demande d'un téléspectateur (demande du téléspectateur)
- Avant CloudFront de transmettre une demande à l'origine (demande d'origine)
- Quand CloudFront reçoit une réponse de l'origine (réponse d'origine)
- Before CloudFront renvoie la réponse au spectateur (réponse du spectateur)

Si vous l'utilisez AWS WAF, la demande du visualiseur Lambda @Edge est exécutée une fois les AWS WAF règles appliquées.

Pour plus d'informations, consultez Utilisation des demandes et des réponses et Structure d'événement Lambda@Edge.

Comment utiliser Lambda@Edge

Le traitement Lambda @Edge peut être utilisé à de nombreuses fins dans votre CloudFront distribution Amazon, comme dans les exemples suivants :

- Une fonction Lambda peut inspecter les cookies et réécrire les URL afin que les utilisateurs puissent consulter les différentes versions d'un site à des fins de test. A/B
- CloudFront peuvent renvoyer différents objets aux spectateurs en fonction de l'appareil qu'ils utilisent en vérifiant l'`User-Agent`en-tête, qui inclut des informations sur les appareils. Par exemple, ils CloudFront peuvent renvoyer différentes images en fonction de la taille de l'écran de leur appareil. De même, la fonction peut prendre en compte la valeur de l'`Refererr`en-tête et CloudFront renvoyer les images aux robots ayant la résolution la plus faible disponible.
- Ou, vous pouvez vérifier les cookies pour d'autres critères. Par exemple, sur un site Web de vente au détail qui vend des vêtements, si vous utilisez des cookies pour indiquer la couleur choisie par un utilisateur pour une veste, une fonction Lambda peut modifier la demande afin de CloudFront renvoyer l'image d'une veste dans la couleur sélectionnée.
- Une fonction Lambda peut générer des réponses HTTP lorsque des événements de demande d' CloudFront utilisateur ou de demande d'origine se produisent.
- Une fonction peut inspecter les en-têtes ou les jetons d'autorisation et insérer un en-tête pour contrôler l'accès à votre contenu avant de CloudFront transmettre la demande à votre origine.
- Une fonction Lambda peut également effectuer des appels réseau à des ressources externes pour confirmer les informations d'identification utilisateur, ou récupérer du contenu supplémentaire pour personnaliser une réponse.

Pour plus d'informations, avec un exemple de code à l'appui, consultez Exemples de fonctions Lambda@Edge.

Pour plus d'informations sur la configuration de Lambda@Edge dans la console, consultez Didacticiel : création d'une fonction Lambda@Edge basique (console).

Mise en route des fonctions Lambda@Edge (console)

Avec Lambda @Edge, vous pouvez utiliser des CloudFront déclencheurs pour appeler une fonction Lambda. Lorsque vous associez une CloudFront distribution à une fonction Lambda, CloudFront intercepte les demandes et les réponses à des emplacements CloudFront périphériques et exécute la fonction. Les fonctions Lambda peuvent améliorer la sécurité ou personnaliser des informations à proximité de vos utilisateurs, afin d'améliorer les performances.

La liste suivante fournit un aperçu de base de la création et de l'utilisation de fonctions Lambda avec. CloudFront

Présentation : Création et utilisation de fonctions Lambda avec CloudFront

1. Créez une fonction Lambda dans la région USA Est (Virginie du Nord).
2. Enregistrez et publiez une version numérotée de la fonction.

   Si vous souhaitez modifier la fonction, vous devez modifier la version $LATEST de la fonction dans la région USA Est (Virginie du Nord). Ensuite, avant de le configurer pour qu'il fonctionne CloudFront, vous publiez une nouvelle version numérotée.
3. Associez la fonction à une CloudFront distribution et à un comportement de cache. Spécifiez ensuite un ou plusieurs CloudFront événements (déclencheurs) à l'origine de l'exécution de la fonction. Par exemple, vous pouvez créer un déclencheur pour que la fonction s'exécute lorsqu'elle CloudFront reçoit une demande d'un utilisateur.
4. Lorsque vous créez un déclencheur, Lambda crée des réplicas de la fonction dans les emplacements AWS à travers le monde.

> **Tip**
>
> Pour plus d'informations, consultez les sections Création et mise à jour de fonctions, structure d'événement et ajout de CloudFront déclencheurs. Vous pouvez également trouver d'autres idées et obtenir des exemples de code dans Exemples de fonctions Lambda@Edge.

Pour accéder à un didacticiel étape par étape, consultez la rubrique suivante :

Rubriques

- Didacticiel : création d'une fonction Lambda@Edge basique (console)

Didacticiel : création d’une fonction Lambda@Edge basique (console)

Ce didacticiel explique comment démarrer avec Lambda @Edge en créant et en configurant un exemple de Node.js fonction qui s'exécute dans. CloudFront Cet exemple ajoute des en-têtes de sécurité HTTP à une réponse lors de la CloudFront récupération d'un fichier. (Cette opération peut améliorer la sécurité et la confidentialité d’un site web.)

Vous n’avez pas besoin d’avoir un site web pour suivre ce didacticiel. Cependant, lorsque vous choisissez de créer votre propre solution Lambda@Edge, vous suivez des étapes similaires et sélectionnez les mêmes options.

Rubriques

- Étape 1 : Inscrivez-vous à un Compte AWS
- Étape 2 : Création d'une CloudFront distribution
- Étape 3 : créer votre fonction
- Étape 4 : ajouter un CloudFront déclencheur pour exécuter la fonction
- Étape 5 : vérifier l’exécution de la fonction
- Étape 6 : résoudre les problèmes
- Étape 7 : nettoyer votre exemple de ressources
- Informations connexes

Étape 1 : Inscrivez-vous à un Compte AWS

Si vous ne l’avez pas encore fait, créez un Compte AWS. Pour plus d’informations, consultez Inscrivez-vous pour un Compte AWS.

Étape 2 : Création d'une CloudFront distribution

Avant de créer l'exemple de fonction Lambda @Edge, vous devez disposer d'un CloudFront environnement avec lequel travailler et qui inclut une origine à partir de laquelle diffuser le contenu.

Dans cet exemple, vous créez une CloudFront distribution qui utilise un compartiment Amazon S3 comme origine de la distribution. Si vous avez déjà un environnement à utiliser, vous pouvez ignorer cette étape.

Pour créer une CloudFront distribution avec une origine Amazon S3

1. Créez un compartiment Amazon S3 avec un fichier ou deux, par exemple des fichiers image, comme exemples de contenu. Pour obtenir de l'aide, suivez les étapes dans Chargement de votre contenu sur Amazon S3. Assurez-vous de définir des autorisations pour accorder l'accès public en lecture sur les objets de votre compartiment.
2. Créez une CloudFront distribution et ajoutez votre compartiment S3 comme origine, en suivant les étapes décrites dans Créer une distribution CloudFront Web. Si vous avez déjà une distribution, vous pouvez, au lieu de cela, ajouter le compartiment en tant qu'origine pour cette distribution.

> **Tip**
>
> Notez votre ID de distribution. Plus loin dans ce didacticiel, lorsque vous ajoutez un CloudFront déclencheur pour votre fonction, vous devez choisir l'ID de votre distribution dans une liste déroulante, par exemple,. `E653W22221KDDL`

Étape 3 : créer votre fonction

Au cours de cette étape, vous créez une fonction Lambda à partir d'un modèle de plan dans la console Lambda. La fonction ajoute du code pour mettre à jour les en-têtes de sécurité dans votre distribution CloudFront.

Pour créer une fonction Lambda

1. Connectez-vous à la AWS Lambda console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/lambda/.

> **Important**
>
> Assurez-vous que vous êtes dans le US-East-1 (Virginie du Nord) Région AWS (us-east-1). Vous devez être dans cette région pour créer des fonctions Lambda@Edge.

2. Choisissez Créer une fonction.
3. Sur la page Créer une fonction, choisissez Utiliser un plan, puis filtrez les CloudFront plans en les saisissant **`cloudfront`** dans le champ de recherche.

> **Note**
>
> CloudFront les plans ne sont disponibles que dans la région US-East-1 (Virginie du Nord) (us-east-1).

4. Choisissez le plan Modifier l'en-tête de réponse HTTP comme modèle pour votre fonction.
5. Entrez les informations suivantes sur votre fonction :
   - Nom de la fonction : entrez un nom pour votre fonction.
   - Rôle d'exécution : choisissez la façon de définir les autorisations pour votre fonction. Pour utiliser le modèle de politique d'autorisation de base recommandé par Lambda @Edge, choisissez Create a new role from AWS policy templates.
   - Nom du rôle : entrez un nom pour le rôle créé par le modèle de stratégie.
   - Modèles de politique — Lambda ajoute automatiquement le modèle de stratégie Basic Lambda @Edge permissions parce que vous avez choisi un CloudFront plan comme base pour votre fonction. Ce modèle de politique ajoute des autorisations de rôle d'exécution qui CloudFront permettent d'exécuter votre fonction Lambda pour vous dans le CloudFront monde entier. Pour plus d'informations, consultez Définition des autorisations et rôles IAM pour Lambda@Edge.
6. Dans le bas de la page, choisissez Créer une fonction.
7. Dans le volet Déployer sur Lambda@Edge qui apparaît, choisissez Annuler. (Pour ce didacticiel, vous devez modifier le code de la fonction avant de déployer la fonction sur Lambda@Edge.)
8. Faites défiler la page jusqu'à la section Source du code.
9. Remplacez le code de modèle par une fonction qui modifie les en-têtes de sécurité renvoyés par votre origine. Par exemple, vous pouvez utiliser du code tel que :

```
'use strict';
export const handler = (event, context, callback) => {

    //Get contents of response
    const response = event.Records[0].cf.response;
    const headers = response.headers;

    //Set new headers
    headers['strict-transport-security'] = [{key: 'Strict-Transport-Security',
 value: 'max-age= 63072000; includeSubdomains; preload'}];
```

```
    headers['content-security-policy'] = [{key: 'Content-Security-Policy', value:
 "default-src 'none'; img-src 'self'; script-src 'self'; style-src 'self'; object-
src 'none'"}];
    headers['x-content-type-options'] = [{key: 'X-Content-Type-Options', value:
 'nosniff'}];
    headers['x-frame-options'] = [{key: 'X-Frame-Options', value: 'DENY'}];
    headers['x-xss-protection'] = [{key: 'X-XSS-Protection', value: '1;
 mode=block'}];
    headers['referrer-policy'] = [{key: 'Referrer-Policy', value: 'same-origin'}];

    //Return modified response
    callback(null, response);
};
```

10. Choisissez Fichier, puis Enregistrer pour enregistrer votre code mis à jour.
11. Choisissez Déployer.

Passez à la section suivante pour ajouter un CloudFront déclencheur permettant d'exécuter la fonction.

Étape 4 : ajouter un CloudFront déclencheur pour exécuter la fonction

Maintenant que vous disposez d'une fonction Lambda pour mettre à jour les en-têtes de sécurité, configurez le CloudFront déclencheur pour exécuter votre fonction afin d'ajouter les en-têtes dans toute réponse CloudFront reçue de l'origine de votre distribution.

Pour configurer le CloudFront déclencheur de votre fonction

1. Dans la console Lambda, sur la page Présentation de la fonction, choisissez Ajouter un déclencheur.
2. Pour la configuration du déclencheur, choisissez CloudFront.
3. Choisissez Déployer sur Lambda@Edge.
4. Dans le volet Deploy to Lambda @Edge, sous Configurer le CloudFront déclencheur, entrez les informations suivantes :

   - Distribution : ID de CloudFront distribution à associer à votre fonction. Dans la liste déroulante, choisissez l’ID de distribution.
   - Comportement de cache : le comportement de cache à utiliser avec le déclencheur. Pour cet exemple, laissez la valeur définie sur *, qui correspond au comportement de cache par défaut

de votre distribution. Pour plus d'informations, consultez Paramètres de comportement du cache dans la rubrique Référence de tous les paramètres de distribution.

- CloudFront event — Le déclencheur qui indique le moment où votre fonction s'exécute. La fonction d'en-têtes de sécurité doit être exécutée chaque fois qu'une réponse est CloudFront renvoyée depuis l'origine. Dans la liste déroulante, choisissez Réponse de l'origine. Pour plus d'informations, consultez Ajout de déclencheurs pour une fonction Lambda@Edge.

5. Cochez la case Confirmer le déploiement sur Lambda@Edge.
6. Choisissez Déployer pour ajouter le déclencheur et répliquer la fonction dans le monde AWS entier.
7. Attendez que la réplication de la fonction soit terminée. Cela prend généralement plusieurs minutes.

   Vous pouvez vérifier si la réplication est terminée en accédant à la console CloudFront et en visualisant votre distribution. Attendez que l'état de la distribution passe de Déploiement à une date et une heure, ce qui indique que votre fonction a été répliquée. Pour vérifier que la fonction s'exécute correctement, suivez les étapes de la section suivante.

Étape 5 : vérifier l'exécution de la fonction

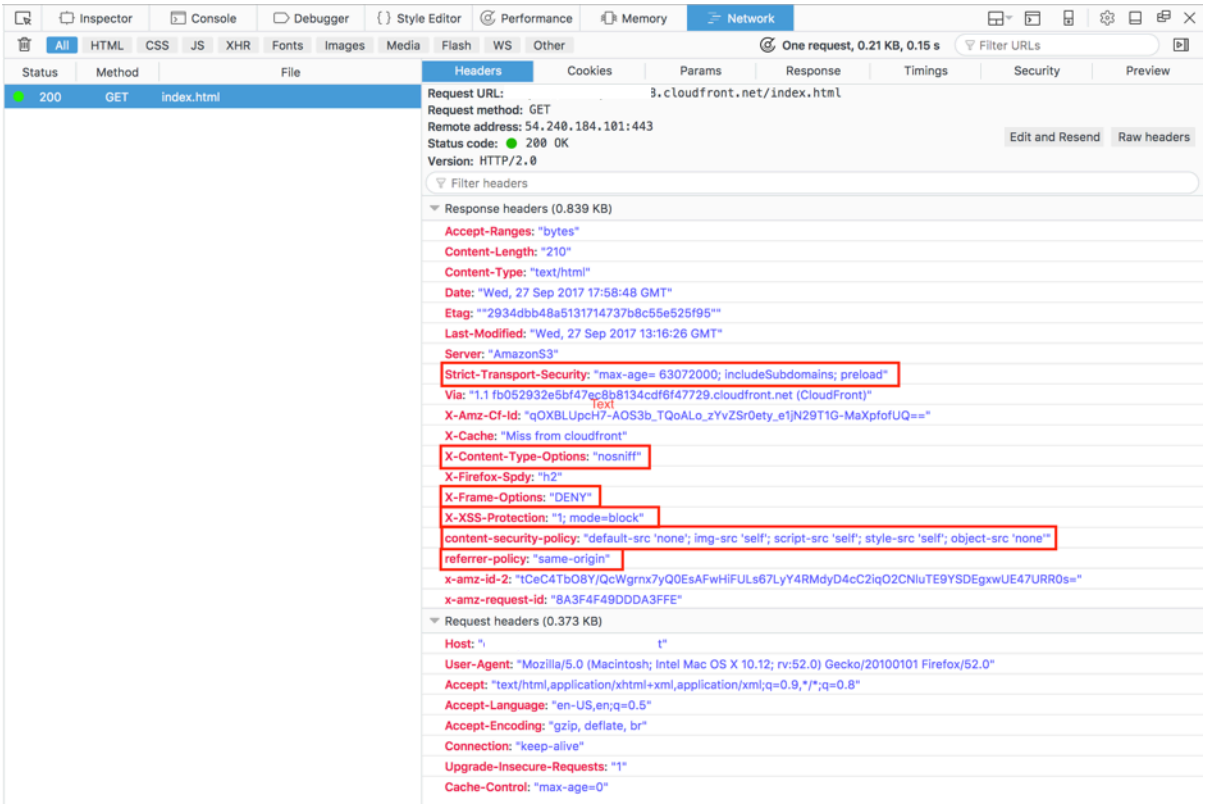
Maintenant que vous avez créé votre fonction Lambda et configuré un déclencheur pour l'exécuter pour une CloudFront distribution, assurez-vous que la fonction répond à vos attentes. Dans cet exemple, vous vérifiez les en-têtes HTTP CloudFront renvoyés pour vous assurer que les en-têtes de sécurité ont été ajoutés.

Pour vérifier que votre fonction Lambda@Edge ajoute des en-têtes de sécurité

1. Dans un navigateur, entrez l'URL d'un fichier dans votre compartiment S3. Par exemple, vous pouvez utiliser une URL similaire à `https://d111111abcdef8.cloudfront.net/image.jpg`.

   Pour plus d'informations sur le nom de CloudFront domaine à utiliser dans l'URL du fichier, consultezPersonnalisez le format d'URL pour les fichiers dans CloudFront.
2. Ouvrez la barre d'outils Web Developer de votre navigateur. Par exemple, dans la fenêtre de votre navigateur dans Chrome, ouvrez le menu contextuel, puis choisissez Inspecter.
3. Choisissez l'onglet Network (Réseau).
4. Rechargez la page pour afficher votre image, puis choisissez une demande HTTP dans le volet de gauche. Vous voyez les en-têtes HTTP s'afficher dans un volet distinct.

5. Parcourez la liste des en-têtes HTTP pour vérifier que les en-têtes de sécurité attendus sont inclus dans la liste. Par exemple, vous pourrez peut-être voir des en-têtes similaires à ceux affichés dans la capture d'écran suivante.



Si les en-têtes de sécurité sont inclus dans votre liste d'en-têtes, cela signifie que vous avez créé avec succès votre première fonction Lambda@Edge. En cas d'erreur de CloudFront retour ou d'autres problèmes, passez à l'étape suivante pour résoudre les problèmes.

Étape 6 : résoudre les problèmes

Si elle CloudFront renvoie des erreurs ou n'ajoute pas les en-têtes de sécurité comme prévu, vous pouvez étudier l'exécution de votre fonction en consultant CloudWatch Logs. Veillez à utiliser les journaux stockés à l' AWS emplacement le plus proche de l'endroit où la fonction est exécutée.

Par exemple, si vous consultez le fichier depuis Londres, essayez de remplacer la région dans la CloudWatch console par Europe (Londres).

Pour examiner les CloudWatch journaux de votre fonction Lambda @Edge

1. Connectez-vous à la CloudWatch console Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.

2. Modifiez Région en spécifiant l'emplacement qui est montré lorsque vous affichez le fichier dans votre navigateur. C'est là que la fonction s'exécute.
3. Dans le volet de gauche, choisissez Logs (Journaux) pour afficher les journaux de votre distribution.

Pour plus d'informations, consultez Surveillez CloudFront les métriques avec Amazon CloudWatch.

Étape 7 : nettoyer votre exemple de ressources

Si vous avez créé un compartiment et une CloudFront distribution Amazon S3 uniquement pour ce didacticiel, supprimez les AWS ressources que vous avez allouées afin de ne plus payer de frais. Une fois que vous avez supprimé vos AWS ressources, le contenu que vous avez ajouté n'est plus disponible.

Tâches

- Supprimer le compartiment S3
- Supprimer la fonction Lambda
- Supprimer la CloudFront distribution

Supprimer le compartiment S3

Avant de supprimer votre compartiment Amazon S3, assurez-vous que la journalisation est désactivée pour le compartiment. Dans le cas contraire, AWS continue d'écrire des journaux dans votre compartiment lorsque vous le supprimez.

Pour désactiver la journalisation pour un compartiment

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Sélectionnez le compartiment, puis choisissez Properties (Propriétés).
3. Dans Properties (Propriétés), choisissez Logging (Journalisation).
4. Désactivez la case à cocher Activé.
5. Choisissez Enregistrer.

Vous pouvez maintenant supprimer votre compartiment. Pour plus d'informations, consultez Suppression d'un compartiment dans le Guide de l'utilisateur de la console Amazon Simple Storage Service.

Supprimer la fonction Lambda

Pour obtenir les instructions permettant de supprimer l'association à la fonction Lambda et, éventuellement, la fonction elle-même, consultez Suppression des fonctions et des réplicas Lambda@Edge.

Supprimer la CloudFront distribution

Avant de supprimer une CloudFront distribution, vous devez la désactiver. Une distribution désactivée n'est plus fonctionnelle et n'accumule pas de frais. Vous pouvez activer une distribution désactivée à tout moment. Une fois que vous avez supprimé une distribution désactivée, celle-ci n'est plus disponible.

Pour désactiver et supprimer une CloudFront distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution que vous souhaitez désactiver, puis choisissez Désactiver).
3. Lorsque vous serez invité à confirmer l'opération, choisissez Oui, désactiver.
4. Sélectionnez la distribution désactivée, puis choisissez Supprimer.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Oui, supprimer.

Informations connexes

Maintenant que vous avez une idée générale de la manière dont les fonctions Lambda@Edge s'exécutent, lisez les documents suivants pour en savoir plus :

- Exemples de fonctions Lambda@Edge
- Bonnes pratiques de conception Lambda @Edge
- Réduction de la latence et transfert du calcul vers la périphérie avec Lambda @Edge

Définition des autorisations et rôles IAM pour Lambda@Edge

Pour configurer Lambda@Edge, vous devez disposer des autorisations et des rôles IAM pour AWS Lambda :

- Autorisations IAM : ces autorisations vous permettent de créer votre fonction Lambda et de l'associer CloudFront à votre distribution.

- Un rôle d'exécution de fonction Lambda (rôle IAM) : les principaux de service Lambda assument ce rôle pour exécuter votre fonction.
- Service-linked rôles pour Lambda @Edge — Les rôles liés aux services permettent à des utilisateurs spécifiques de Services AWS répliquer des fonctions Lambda vers des fichiers journaux Régions AWS et de les utiliser. CloudWatch CloudFront

Autorisations IAM requises pour associer les fonctions Lambda @Edge aux distributions CloudFront

Outre les autorisations IAM dont vous avez besoin pour Lambda, vous avez besoin des autorisations suivantes pour associer les fonctions Lambda aux distributions : CloudFront

- `lambda:GetFunction` : accorde l'autorisation d'obtenir les informations de configuration de votre fonction Lambda ainsi qu'une URL pré-signée pour télécharger un fichier `.zip` contenant la fonction.
- `lambda:EnableReplication*` : accorde une autorisation à la politique de ressource afin que le service de réplication Lambda puisse récupérer le code et la configuration de la fonction.
- `lambda:DisableReplication*` : accorde une autorisation à la politique de ressource afin que le service de réplication Lambda puisse supprimer la fonction.

> **Important**
>
> Vous devez ajouter l'astérisque (`*`) à la fin des actions `lambda:EnableReplication*` et `lambda:DisableReplication*`.

- Pour la ressource, spécifiez l'ARN de la version de fonction que vous souhaitez exécuter lorsqu'un CloudFront événement se produit, comme dans l'exemple suivant :

  `arn:aws:lambda:us-east-1:123456789012:function:TestFunction:2`

- `iam:CreateServiceLinkedRole`— Accorde l'autorisation de créer un rôle lié à un service que Lambda @Edge utilise pour répliquer les fonctions Lambda. CloudFront Après avoir configuré Lambda@Edge pour la première fois, le rôle lié au service est créé automatiquement pour vous. Il n'est pas nécessaire d'ajouter cette autorisation aux autres distributions qui utilisent Lambda@Edge.

- `cloudfront:UpdateDistribution` ou `cloudfront:CreateDistribution` : accorde l'autorisation de mettre à jour ou de créer une distribution.

Pour plus d'informations, consultez les rubriques suivantes :

- Gestion des identités et des accès pour Amazon CloudFront
- Autorisations d'accès aux ressources Lambda dans le Guide du développeur AWS Lambda

Rôle d'exécution de fonction pour les principaux de service

Vous devez créer un rôle IAM que les principaux de service `lambda.amazonaws.com` et `edgelambda.amazonaws.com` peuvent assumer lorsqu'ils exécutent votre fonction.

> **Tip**
>
> Lorsque vous créez votre fonction dans la console Lambda, vous pouvez choisir de créer un nouveau rôle d'exécution à l'aide d'un modèle de AWS politique. Cette étape ajoute automatiquement les autorisations Lambda@Edge requises pour exécuter votre fonction. Consultez l'étape 5 du Didacticiel : création d'une fonction Lambda@Edge simple.

Pour plus d'informations sur la création manuelle d'un rôle IAM, consultez Création des rôles et association des politiques (console) dans le Guide de l'utilisateur IAM.

Example Exemple : stratégie d'approbation du rôle

Vous pouvez ajouter ce rôle sous l'onglet Relations d'approbation dans la console IAM. N'ajoutez pas cette politique sous l'onglet Autorisations.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": [
               "lambda.amazonaws.com",
               "edgelambda.amazonaws.com"
            ]
         },
         "Action": "sts:AssumeRole"
```

```
        }
    ]
}
```

Pour plus d'informations sur les autorisations que vous devez associer au rôle d'exécution, consultez Autorisations d'accès aux ressources Lambda dans le Guide du développeur AWS Lambda .

Remarques

- Par défaut, chaque fois qu'un CloudFront événement déclenche une fonction Lambda, les données sont écrites dans Logs. CloudWatch Si vous souhaitez utiliser ces journaux, le rôle d'exécution doit être autorisé à écrire des données dans les CloudWatch journaux. Vous pouvez utiliser le AWSLambdaBasicExecutionRole prédéfini pour accorder l'autorisation nécessaire au rôle d'exécution.

  Pour plus d'informations sur CloudWatch les journaux, consultezthe section called "Journaux des fonctions de périphérie".
- Si le code de votre fonction Lambda accède à d'autres AWS ressources, telles que la lecture d'un objet depuis un compartiment S3, le rôle d'exécution doit être autorisé pour effectuer cette action.

Service-linked rôles pour Lambda @Edge

Lambda@Edge utilise des rôles liés à un service IAM. Un rôle lié à un service est un type unique de rôle IAM directement lié à un service. Service-linked les rôles sont prédéfinis par le service et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Lambda@Edge utilise les rôles liés à un service IAM suivants :

- AWSServiceRoleForLambdaReplicator – Lambda@Edge utilise ce rôle pour autoriser Lambda@Edge à répliquer des fonctions vers Régions AWS.

  Lorsque vous ajoutez un déclencheur Lambda @Edge pour la première fois CloudFront, un rôle nommé AWSServiceRoleForLambdaReplicator est créé automatiquement pour permettre à Lambda @Edge de répliquer des fonctions sur. Régions AWS Ce rôle est obligatoire pour utiliser les fonctions Lambda@Edge. L'ARN du rôle AWSServiceRoleForLambdaReplicator ressemble à l'exemple suivant :

```
arn:aws:iam::123456789012:role/aws-service-role/
replicator.lambda.amazonaws.com/AWSServiceRoleForLambdaReplicator
```

- AWSServiceRoleForCloudFrontLogger— CloudFront utilise ce rôle pour transférer les fichiers journaux dans CloudWatch. Vous pouvez utiliser des fichiers journaux pour corriger les erreurs de validation Lambda@Edge.

  Le AWSServiceRoleForCloudFrontLogger rôle est créé automatiquement lorsque vous ajoutez une association de fonctions Lambda @Edge pour permettre de transférer les fichiers CloudFront journaux d'erreurs Lambda @Edge vers. CloudWatch L'ARN pour le rôle AWSServiceRoleForCloudFrontLogger prend la forme suivante :

  ```
  arn:aws:iam::account_number:role/aws-service-role/
  logger.cloudfront.amazonaws.com/AWSServiceRoleForCloudFrontLogger
  ```

Un rôle lié à un service simplifie la configuration et l'utilisation de Lambda@Edge, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Lambda@Edge définit les autorisations de ses rôles liés un service et seul Lambda@Edge peut endosser ces rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Vous ne pouvez pas attacher la politique d'autorisations à une autre entité IAM.

Vous devez supprimer toutes les ressources associées CloudFront ou Lambda @Edge avant de pouvoir supprimer un rôle lié à un service. Cela vous aide à protéger vos ressources Lambda@Edge afin d'éviter la suppression d'un rôle lié à un service qui est encore nécessaire pour accéder à des ressources actives.

Pour plus d'informations sur les rôles liés à un service, consultez Service-linked rôles pour CloudFront.

Service-linked autorisations de rôle pour Lambda @Edge

Lambda@Edge utilise deux rôles liés à un service nommé AWSServiceRoleForLambdaReplicator et AWSServiceRoleForCloudFrontLogger. Les sections suivantes décrivent comment gérer les autorisations pour chacun de ces rôles.

Table des matières

- Service-linked autorisations de rôle pour le réplicateur Lambda
- Service-linked autorisations de rôle pour l' CloudFront enregistreur

Service-linked autorisations de rôle pour le réplicateur Lambda

Ce rôle lié à un service permet à Lambda de répliquer les fonctions Lambda@Edge vers Régions AWS.

Le rôle lié à un service AWSServiceRoleForLambdaReplicator fait confiance au service `replicator.lambda.amazonaws.com` pour endosser le rôle.

La politique d'autorisations du rôle permet à Lambda@Edge de réaliser les actions suivantes sur les ressources spécifiées :

- `lambda:CreateFunction` sur `arn:aws:lambda:*:*:function:*`
- `lambda:DeleteFunction` sur `arn:aws:lambda:*:*:function:*`
- `lambda:DisableReplication` sur `arn:aws:lambda:*:*:function:*`
- `iam:PassRole` sur `all AWS resources`
- `cloudfront:ListDistributionsByLambdaFunction` sur `all AWS resources`

Service-linked autorisations de rôle pour l' CloudFront enregistreur

Ce rôle lié à un service permet de CloudFront transférer des fichiers journaux CloudWatch afin que vous puissiez corriger les erreurs de validation Lambda @Edge.

Le rôle lié à un service AWSServiceRoleForCloudFrontLogger fait confiance au service `logger.cloudfront.amazonaws.com` pour endosser le rôle.

La politique d’autorisations du rôle permet à Lambda@Edge de réaliser les actions suivantes sur les ressources `arn:aws:logs:*:*:log-group:/aws/cloudfront/*` spécifiées :

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:PutLogEvents`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, groupe ou rôle) de supprimer les rôles liés à un service Lambda@Edge. Pour plus d'informations, consultez les autorisations relatives aux Service-linked rôles dans le guide de l'utilisateur IAM.

Création de rôles liés à un service pour Lambda@Edge

Vous n'avez généralement pas besoin de créer manuellement les rôles liés à un service pour Lambda@Edge. Le service crée les rôles automatiquement pour vous dans les scénarios suivants :

- Lorsque vous créez un déclencheur pour la première fois, le service crée le rôle AWSServiceRoleForLambdaReplicator (s'il n'existe pas encore.). Ce rôle permet à Lambda de répliquer les fonctions Lambda@Edge vers Régions AWS.

  Si vous supprimez le rôle lié à un service, le rôle sera à nouveau créé lorsque vous ajouterez un nouveau déclencheur pour Lambda@Edge dans une distribution.
- Lorsque vous mettez à jour ou créez une CloudFront distribution associée à Lambda @Edge, le service crée le AWSServiceRoleForCloudFrontLogger rôle (si le rôle n'existe pas déjà). Ce rôle permet CloudFront de transférer vos fichiers journaux vers CloudWatch.

  Si vous supprimez le rôle lié à un service, le rôle sera créé à nouveau lorsque vous mettrez à jour ou créerez une CloudFront distribution associée à Lambda @Edge.

Pour créer manuellement ces rôles liés à un service, vous pouvez exécuter les commandes suivantes AWS Command Line Interface (AWS CLI) :

Pour créer le AWSServiceRoleForLambdaReplicator rôle

- Exécutez la commande suivante.

```
aws iam create-service-linked-role --aws-service-name
 replicator.lambda.amazonaws.com
```

Pour créer le AWSServiceRoleForCloudFrontLogger rôle

- Exécutez la commande suivante.

```
aws iam create-service-linked-role --aws-service-name
 logger.cloudfront.amazonaws.com
```

Modification des rôles liés à un service Lambda@Edge.

Lambda@Edge ne vous permet pas de modifier les rôles liés à un service AWSServiceRoleForLambdaReplicator ou AWSServiceRoleForCloudFrontLogger. Une fois que le service a créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent y faire référence. Néanmoins, vous pouvez utiliser IAM pour modifier la description du rôle. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Pris en charge Régions AWS pour les rôles liés au service Lambda @Edge

CloudFront prend en charge l'utilisation de rôles liés à un service pour Lambda @Edge dans les domaines suivants : Régions AWS

- USA Est (Virginie du Nord) – `us-east-1`
- USA Est (Ohio) – `us-east-2`
- USA Ouest (Californie du Nord) – `us-west-1`
- USA Ouest (Oregon) – `us-west-2`
- Asie-Pacifique (Mumbai) – `ap-south-1`
- Asie-Pacifique (Séoul) – `ap-northeast-2`
- Asie-Pacifique (Singapour) – `ap-southeast-1`
- Asie-Pacifique (Sydney) – `ap-southeast-2`
- Asie-Pacifique (Tokyo) : `ap-northeast-1`
- Europe (Francfort) – `eu-central-1`
- Europe (Irlande) – `eu-west-1`
- Europe (Londres) – `eu-west-2`
- South America (São Paulo) – `sa-east-1`

Écriture et création d'une fonction Lambda@Edge

Pour utiliser Lambda@Edge, vous devez écrire le code de votre fonction AWS Lambda . Pour vous aider à écrire des fonctions Lambda@Edge, consultez les ressources suivantes :

- Structure d'événement Lambda@Edge : comprenez la structure d'événement à utiliser avec Lambda@Edge.

- Exemples de fonctions Lambda@Edge— Exemples de fonctions, telles que le A/B test et la génération d'une redirection HTTP.

Le modèle de programmation pour utiliser Node.js Python avec Lambda @Edge est le même que pour utiliser Lambda dans un. Région AWSPour plus d'informations, voir Création de fonctions Lambda avec Node.js ou Création de fonctions Lambda avec Python dans le Guide du développeur.AWS Lambda

Dans votre fonction Lambda@Edge, insérez le paramètre `callback` et renvoyez l'objet applicable pour les événements de demande ou de réponse :

- Événements de demande – Incluez l'objet `cf.request` dans la réponse.

  Si vous générez une réponse, incluez l'objet `cf.response` dans la réponse. Pour plus d'informations, consultez Génération de réponses HTTP dans les déclencheurs de demande.
- Événements de réponse – Incluez l'objet `cf.response` dans la réponse.

Après avoir écrit votre propre code ou utilisé l'un des exemples, vous créez la fonction dans Lambda. Pour créer une fonction ou modifier une fonction existante, consultez les rubriques suivantes :

Rubriques

- Création d'une fonction Lambda@Edge
- Modification d'une fonction Lambda

Après avoir créé la fonction dans Lambda, vous configurez Lambda pour qu'elle exécute la fonction en fonction d' CloudFront événements spécifiques, appelés déclencheurs. Pour plus d'informations, consultez Ajout de déclencheurs pour une fonction Lambda@Edge.

Création d'une fonction Lambda@Edge

AWS Lambda Pour configurer l'exécution de fonctions Lambda basées sur des CloudFront événements, suivez cette procédure.

Pour créer une fonction Lambda@Edge

1. Connectez-vous à la AWS Lambda console Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.

2. Si vous avez déjà une ou plusieurs fonctions Lambda, choisissez Create function (Créer fonction).

   Si vous n'avez aucune fonction, choisissez Mise en route.
3. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).
4. Créez une fonction à l'aide de votre propre code ou en partant d'un plan CloudFront .

   - Pour créer une fonction à l'aide de votre propre code, choisissez Créer à partir de zéro.
   - Pour afficher une liste de plans pour CloudFront, saisissez cloudfront dans le champ de filtre, puis choisissez Entrée.

     Si vous trouvez un plan que vous souhaitez utiliser, choisissez le nom de ce plan.
5. Dans la section Informations de base, spécifiez les valeurs suivantes :

   a. Nom : saisissez le nom de votre fonction.

   b. Rôle : pour démarrer rapidement, choisissez Créer un rôle à partir de modèles. Vous pouvez également sélectionner Choisir un rôle existant ou Créer un rôle personnalisé, puis suivre les invites pour compléter les informations de cette section.

   c. Nom du rôle : entrez un nom pour le rôle.

   d. Modèles de stratégies : choisissez Autorisations Lambda de périphérique standard.
6. Si vous avez choisi Créer à partir de zéro à l'étape 4, passez directement à l'étape 7.

   Si vous avez choisi un plan à l'étape 4, vous pouvez utiliser la section cloudfront pour créer un déclencheur, qui associe cette fonction à un cache dans une CloudFront distribution et un CloudFront événement. Pour l'instant, nous vous recommandons de choisir Supprimer, afin qu'il n'y ait pas de déclencheur pour la fonction lorsqu'elle sera créée. Vous pourrez ajouter des déclencheurs par la suite.

   > **Tip**
   >
   > Nous vous recommandons de tester et déboguer la fonction avant d'ajouter des déclencheurs. Si vous ajoutez un déclencheur maintenant, la fonction s'exécutera dès que vous la créerez, qu'elle aura fini de se répliquer AWS dans le monde entier et que la distribution correspondante sera déployée.
7. Choisissez Créer une fonction.

Lambda crée deux versions de votre fonction : $LATEST et Version 1. Vous pouvez modifier uniquement la version $LATEST, mais la console affiche initialement la version 1.

8. Pour modifier la fonction, choisissez Version 1 en haut de la page, sous l'ARN de la fonction. Puis, dans l'onglet Versions, choisissez $LATEST. (Si vous avez quitté la fonction, puis êtes revenu à celle-ci, le bouton est appelé Qualificateurs.)
9. Dans l'onglet Configuration, choisissez le Type d'entrée de code applicable. Ensuite, suivez les instructions pour modifier ou charger votre code.
10. Pour Exécution, choisissez la valeur en fonction du code de votre fonction.
11. Dans la section Balises, ajoutez les éventuelles balises applicables.
12. Choisissez Actions, puis Publier une nouvelle version.
13. Saisissez la description de la nouvelle version de la fonction.
14. Choisissez Publish.
15. Testez et déboguez la fonction. Pour plus d'informations sur les tests de la console Lambda, consultez Invoquer une fonction Lambda avec la console dans le Guide du développeur AWS Lambda .
16. Lorsque vous êtes prêt à exécuter la fonction pour des CloudFront événements, publiez une autre version et modifiez la fonction pour ajouter des déclencheurs. Pour plus d'informations, consultez Ajout de déclencheurs pour une fonction Lambda@Edge.

Modification d'une fonction Lambda

Après avoir créé une fonction Lambda@Edge, vous pouvez utiliser la console Lambda pour la modifier.

> **Remarques**
>
> - La version d'origine est étiquetée $LATEST.
> - Vous ne pouvez modifier que la version $LATEST.
> - Chaque fois que vous modifiez la version $LATEST, vous devez publier une nouvelle version numérotée.
> - Vous ne pouvez pas créer de déclencheurs pour $LATEST.

- Lorsque vous publiez une nouvelle version d'une fonction, Lambda ne copie pas automatiquement les déclencheurs à partir de la version précédente vers la nouvelle version. Vous devez reproduire les déclencheurs pour la nouvelle version.
- Lorsque vous ajoutez un déclencheur pour un CloudFront événement à une fonction, s'il existe déjà un déclencheur pour la même distribution, le même comportement de cache et le même événement pour une version antérieure de la même fonction, Lambda supprime le déclencheur de la version précédente.
- Après avoir mis à jour une CloudFront distribution, par exemple en ajoutant des déclencheurs, vous devez attendre que les modifications se propagent aux emplacements périphériques pour que les fonctions que vous avez spécifiées dans les déclencheurs fonctionnent.

Pour modifier une fonction Lambda

1. Connectez-vous à la AWS Lambda console Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Dans la liste des fonctions, choisissez le nom de la fonction.

   Par défaut, la console affiche la version $LATEST. Vous pouvez consulter les versions précédentes (choisissez Qualificateurs), mais vous ne pouvez modifier que $ LATEST.
4. Dans l'onglet Code, pour Code entry type (Type d'entrée de code), choisissez de modifier le code dans le navigateur, de charger un fichier .zip ou de charger un fichier depuis Amazon S3.
5. Choisissez Enregistrer ou Enregistrer et tester.
6. Choisissez Actions, puis Publish new version (Publier nouvelle version).
7. Dans la boîte de dialogue Publier la nouvelle version à partir de $LATEST, indiquez une description de la nouvelle version. Cette description s'affiche dans la liste des versions, accompagnée d'un numéro de version généré automatiquement.
8. Choisissez Publish.

   La nouvelle version devient automatiquement la version la plus récente. Le numéro de version s’affiche dans la zone Version dans l’angle supérieur gauche de la page.

> **Note**
>
> Si vous n'avez pas encore ajouté de déclencheurs pour votre fonction, consultez Ajout de déclencheurs pour une fonction Lambda@Edge.

9. Choisissez l'onglet Déclencheurs.
10. Choisissez Add trigger (Ajouter déclencheur).
11. Dans la boîte de dialogue Add trigger (Ajouter déclencheur), choisissez la zone en pointillé, puis CloudFront.

> **Note**
>
> Si vous avez déjà créé un ou plusieurs déclencheurs pour une fonction, CloudFront c'est le service par défaut.

12. Spécifiez les valeurs suivantes pour indiquer le moment où vous voulez que la fonction Lambda s'exécute.

    a. ID de distribution : choisissez l'ID de la distribution que vous souhaitez ajouter au déclencheur.

    b. Comportement du cache : choisissez le comportement de cache qui spécifie les objets sur lesquels vous souhaitez exécuter la fonction.

    c. CloudFront event — Choisissez l' CloudFront événement à l'origine de l'exécution de la fonction.

    d. Activer le déclencheur et répliquer : cochez cette case pour que Lambda effectue une réplication globale de la fonction vers les Régions AWS .

13. Sélectionnez Soumettre.
14. Pour ajouter d'autres déclencheurs pour cette fonction, répétez les étapes 10 à 13.

Pour plus d'informations sur les tests et le débogage de la console Lambda, consultez Invoquer une fonction Lambda avec la console dans le Guide du développeur AWS Lambda .

Lorsque vous êtes prêt à exécuter la fonction pour des CloudFront événements, publiez une autre version et modifiez la fonction pour ajouter des déclencheurs. Pour plus d'informations, consultez Ajout de déclencheurs pour une fonction Lambda@Edge.

Ajout de déclencheurs pour une fonction Lambda@Edge

Un déclencheur Lambda @Edge est une combinaison d'une CloudFront distribution, d'un comportement de cache et d'un événement qui entraîne l'exécution d'une fonction. Par exemple, vous pouvez créer un déclencheur qui entraîne l'exécution de la fonction lorsqu'un utilisateur CloudFront reçoit une demande concernant un comportement de cache spécifique que vous avez configuré pour votre distribution. Vous pouvez spécifier un ou plusieurs CloudFront déclencheurs.

> **Tip**
>
> Lorsque vous créez une CloudFront distribution, vous spécifiez des paramètres qui indiquent CloudFront comment répondre lorsqu'elle reçoit différentes demandes. Les paramètres par défaut correspondent au comportement de cache par défaut pour la distribution. Vous pouvez configurer des comportements de cache supplémentaires qui définissent la manière dont il CloudFront répond dans des circonstances spécifiques, par exemple lorsqu'il reçoit une demande pour un type de fichier spécifique. Pour plus d'informations, consultez Paramètres de comportement du cache.

Lorsque vous créez pour la première fois une fonction Lambda, vous ne pouvez spécifier qu'un seul déclencheur. Vous pouvez ajouter d'autres déclencheurs à la même fonction ultérieurement en utilisant la console Lambda ou en modifiant la distribution dans la CloudFront console.

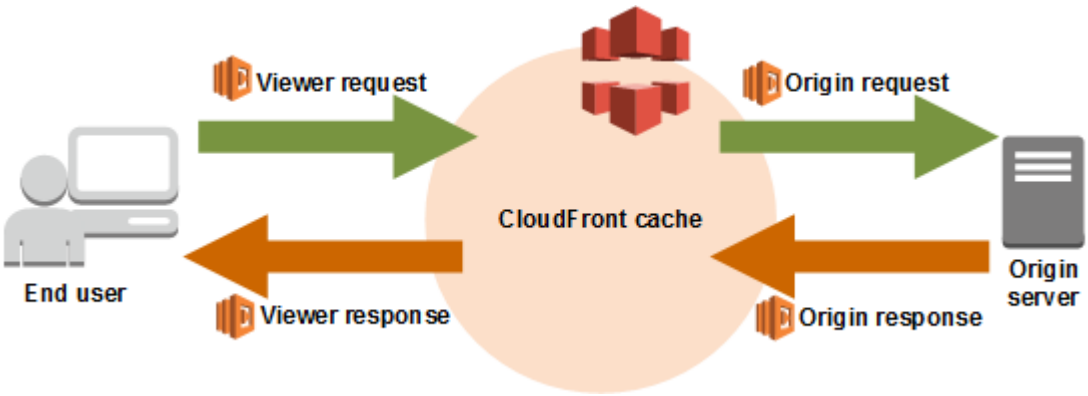
- La console Lambda fonctionne bien si vous souhaitez ajouter d'autres déclencheurs à une fonction pour la même CloudFront distribution.
- La CloudFront console peut être meilleure si vous souhaitez ajouter des déclencheurs pour plusieurs distributions, car il est plus facile de trouver la distribution que vous souhaitez mettre à jour. Vous pouvez également mettre à jour d'autres CloudFront paramètres en même temps.

Rubriques

- CloudFront événements pouvant déclencher une fonction Lambda @Edge
- Choix de l'événement qui déclenche la fonction
- Ajout de déclencheurs à une fonction Lambda@Edge

CloudFront événements pouvant déclencher une fonction Lambda @Edge

Pour chaque comportement de cache dans une CloudFront distribution Amazon, vous pouvez ajouter jusqu'à quatre déclencheurs (associations) qui déclenchent l'exécution d'une fonction Lambda lorsque des CloudFront événements spécifiques se produisent. CloudFront les déclencheurs peuvent être basés sur l'un des quatre CloudFront événements suivants, comme le montre le schéma suivant.



Les CloudFront événements qui peuvent être utilisés pour déclencher les fonctions Lambda @Edge sont les suivants :

Demande utilisateur

La fonction s'exécute lorsqu'elle CloudFront reçoit une demande d'un visualiseur, avant de vérifier si l'objet demandé se trouve dans le CloudFront cache.

La fonction ne s’exécute pas dans les cas suivants :

- Lors de la récupération d’une page d’erreur personnalisée.
- Lorsque redirige CloudFront automatiquement une requête HTTP vers HTTPS (lorsque la valeur de Viewer Protocol Policy est Rediriger HTTP vers HTTPS).

demande à l’origine

La fonction s'exécute uniquement lorsque CloudFront vous transmettez une demande à votre origine. Lorsque l'objet demandé se trouve dans le CloudFront cache, la fonction ne s'exécute pas.

Réponse de l’origine

La fonction s'exécute après avoir CloudFront reçu une réponse de l'origine et avant de mettre en cache l'objet dans la réponse. Notez que la fonction s'exécute même si une erreur est renvoyée de l'origine.

La fonction ne s’exécute pas dans les cas suivants :

- Lorsque le fichier demandé est dans le CloudFront cache et n'a pas expiré.
- Lorsque la réponse est générée à partir d'une fonction qui a été déclenchée par un événement de demande à l'origine.

Réponse utilisateur

La fonction s'exécute avant de renvoyer le fichier demandé à l'utilisateur. Notez que la fonction s'exécute indépendamment du fait que le fichier soit déjà dans le CloudFront cache ou non.

La fonction ne s’exécute pas dans les cas suivants :

- Lorsque l'origine renvoie un code de statut HTTP égal ou supérieur à 400.
- Lorsqu'une page d'erreur personnalisée est renvoyée.
- Lorsque la réponse est générée à partir d'une fonction qui a été déclenchée par un événement de demande utilisateur.
- Lorsque redirige CloudFront automatiquement une requête HTTP vers HTTPS (lorsque la valeur de Viewer Protocol Policy est Rediriger HTTP vers HTTPS).

Lorsque vous ajoutez plusieurs déclencheurs au même comportement de cache, vous pouvez les utiliser pour exécuter la même fonction ou des fonctions différentes pour chaque déclencheur. Vous pouvez associer la même fonction à plusieurs distributions.

> **Note**
>
> Lorsqu'un CloudFront événement déclenche l'exécution d'une fonction Lambda, celle-ci doit se terminer avant de CloudFront pouvoir continuer.
> Par exemple, si une fonction Lambda est déclenchée par un événement de demande d'affichage, elle CloudFront ne renverra pas de réponse au CloudFront visualiseur ni ne transmettra la demande à l'origine tant que la fonction Lambda n'aura pas fini de s'exécuter. Cela signifie que chaque demande qui déclenche une fonction Lambda augmente sa latence. Vous souhaitez ainsi que la fonction s’exécute le plus vite possible.

Choix de l’événement qui déclenche la fonction

Lorsque vous décidez quel CloudFront événement vous souhaitez utiliser pour déclencher une fonction Lambda, tenez compte des points suivants :

Je souhaite CloudFront mettre en cache des objets modifiés par une fonction Lambda

Pour mettre en cache un objet qui a été modifié par une fonction Lambda afin de CloudFront pouvoir le servir depuis l'emplacement périphérique lors de sa prochaine demande, utilisez l'événement de demande d'origine ou de réponse d'origine.

Cela réduit la charge sur l'origine, réduit la latence pour les demandes suivantes et réduit le coût de l'appel de Lambda@Edge sur les demandes suivantes.

Par exemple, si vous souhaitez ajouter, supprimer ou modifier les en-têtes des objets renvoyés par l'origine et que vous souhaitez CloudFront mettre le résultat en cache, utilisez l'événement de réponse d'origine.

Je souhaite que la fonction s’exécute pour chaque demande

Pour exécuter la fonction pour chaque demande CloudFront reçue pour la distribution, utilisez les événements de demande du visualiseur ou de réponse du visualiseur.

Les événements de demande d'origine et de réponse d'origine se produisent uniquement lorsqu'un objet demandé n'est pas mis en cache dans un emplacement périphérique et CloudFront transmet une demande à l'origine.

Je souhaite que la fonction modifie la clé de cache

Pour modifier une valeur que vous utilisez comme base pour la mise en cache, utilisez l’événement demande utilisateur.

Par exemple, si une fonction modifie l'URL pour inclure une abréviation de langue dans le chemin d'accès (par exemple, parce que l'utilisateur a choisi sa langue dans une liste déroulante), utilisez l'événement de demande utilisateur :

- URL dans la demande du lecteur — https://example.com/en/index.html
- URL lorsque la demande provient d'une adresse IP en Allemagne — https://example.com/de/index.html

Vous utilisez également l'événement de demande utilisateur si vous mettez en cache en fonction des cookies ou des en-têtes de demande.

> **Note**
>
> Si la fonction modifie les cookies ou les en-têtes, configurez CloudFront pour transmettre la partie applicable de la demande à l'origine. Pour plus d’informations, consultez les rubriques suivantes :

- Mise en cache de contenu basée sur des cookies
- Mise en cache de contenu basée sur des en-têtes de demandes

La fonction affecte la réponse provenant de l'origine

Pour modifier la demande d'une manière qui affecte la réponse de l'origine, utilisez l'événement demande à l'origine.

En général, la plupart des événements de demande du visiteur ne sont pas transmis à l'origine. CloudFront répond à une demande avec un objet qui se trouve déjà dans le cache périphérique. Si la fonction modifie la demande en fonction d'un événement de demande d'origine, met en CloudFront cache la réponse à la demande d'origine modifiée.

Ajout de déclencheurs à une fonction Lambda@Edge

Vous pouvez utiliser la AWS Lambda console ou la CloudFront console Amazon pour ajouter un déclencheur à votre fonction Lambda @Edge.

Important

Vous ne pouvez créer des déclencheurs que pour les versions numérotées de votre fonction (et non pour le $LATEST).

Lambda console

Pour ajouter des déclencheurs d' CloudFront événements à une fonction Lambda @Edge

1. Connectez-vous à la AWS Lambda console Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).
3. Sur la page Fonctions, choisissez le nom de la fonction pour laquelle vous souhaitez ajouter des déclencheurs.
4. Sur la page Présentation de la fonction, choisissez l'onglet Versions.
5. Choisissez la version à laquelle vous souhaitez ajouter des déclencheurs.

Une fois que vous avez choisi une version, le texte du bouton est remplacé par Version: $LATEST ou Version: numéro de version.

6. Choisissez l'onglet Triggers (Déclencheurs).
7. Choisissez Add trigger (Ajouter déclencheur).
8. Pour la configuration du déclencheur, choisissez Sélectionner une source**`cloudfront`**, entrez, puis choisissez CloudFront.

> **Note**
>
> Si vous avez déjà créé un ou plusieurs déclencheurs, CloudFront c'est le service par défaut.

9. Spécifiez les valeurs suivantes pour indiquer le moment où vous voulez que la fonction Lambda s'exécute.

   a. Distribution : choisissez la distribution que vous souhaitez ajouter au déclencheur.

   b. Comportement du cache : choisissez le comportement de cache qui spécifie les objets sur lesquels vous souhaitez exécuter la fonction.

   > **Note**
   >
   > Si vous spécifiez * pour le comportement de cache, la fonction Lambda se déploie sur le comportement de cache par défaut.

   c. CloudFront event — Choisissez l'CloudFront événement à l'origine de l'exécution de la fonction.

   d. Inclure le corps : cochez cette case si vous souhaitez accéder au corps de la demande dans votre fonction.

   e. Confirmer le déploiement sur Lambda@Edge : cochez cette case pour qu' AWS Lambda réplique la fonction dans les Régions AWS du monde entier.

10. Choisissez Ajouter.

La fonction commence à traiter les demandes relatives aux CloudFront événements spécifiés lorsque la CloudFront distribution mise à jour est déployée. Pour déterminer si une distribution a été déployée, choisissez Distributions dans le panneau de navigation.

Lorsqu'une distribution a été déployée, la valeur de la colonne Statut correspondant à la distribution passe de Déploiement à la date et l'heure du déploiement.

CloudFront console

Pour ajouter des déclencheurs d' CloudFront événements à une fonction Lambda @Edge

1. Obtenez le nom ARN de la fonction Lambda pour laquelle vous voulez ajouter des déclencheurs :

   a. Connectez-vous à la AWS Lambda console Console de gestion AWS et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.

   b. Dans la liste des régions située en haut de la page, choisissez US East (N. Virginia) (USA Est (Virginie du Nord)).

   c. Dans la liste des fonctions, choisissez le nom de la fonction à laquelle vous voulez ajouter des déclencheurs.

   d. Sur la page Présentation de la fonction, choisissez l'onglet Versions et sélectionnez la version numérotée à laquelle vous voulez ajouter des déclencheurs.

   e. Choisissez le bouton Copier l'ARN pour copier l'ARN dans votre presse-papiers. L'ARN de la fonction Lambda ressemble à ceci :

      ```
      arn:aws:lambda:us-east-1:123456789012:function:TestFunction:2
      ```

      Le numéro à la fin (2 dans cet exemple) est le numéro de version de la fonction.

2. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
3. Dans la liste des distributions, choisissez l'ID de la distribution à laquelle vous voulez ajouter des déclencheurs.
4. Choisissez l'onglet Comportements.
5. Sélectionnez le comportement de cache auquel vous souhaitez ajouter des déclencheurs, puis choisissez Modifier.
6. Dans Associations de fonctions, dans la liste Type de fonction, choisissez Lambda@Edge pour exécuter la fonction lors des demandes utilisateur, des réponses utilisateur, des demandes d'origine ou des réponses d'origine.

   Pour plus d'informations, consultez Choix de l'événement qui déclenche la fonction.

7. Dans la zone de texte ARN/Nom de la fonction, collez l'ARN de la fonction Lambda que vous souhaitez exécuter lorsque l'événement choisi se produit. Il s'agit de la valeur que vous avez copiée à partir de la console Lambda.
8. Cochez la case Inclure corps si vous souhaitez accéder au corps de la demande dans votre fonction.

   Si vous souhaitez simplement remplacer le corps de la demande, vous n'avez pas besoin de sélectionner cette option.
9. Pour exécuter la même fonction pour plusieurs types d'événements, répétez les étapes 6 et 7.
10. Cliquez sur Enregistrer les modifications.
11. Pour ajouter des déclencheurs à d'autres comportements de cache pour cette distribution, répétez les étapes 5 à 10.

    La fonction commence à traiter les demandes relatives aux CloudFront événements spécifiés lorsque la CloudFront distribution mise à jour est déployée. Pour déterminer si une distribution a été déployée, choisissez Distributions dans le panneau de navigation. Lorsqu'une distribution a été déployée, la valeur de la colonne Statut correspondant à la distribution passe de Déploiement à la date et l'heure du déploiement.

Test et débogage des fonctions Lambda@Edge

Il est important de tester votre code de fonction Lambda @Edge de manière autonome, pour vous assurer qu'il exécute la tâche prévue, et de réaliser des tests d'intégration pour vous assurer que la fonction fonctionne correctement avec. CloudFront

Au cours des tests d'intégration ou après le déploiement de votre fonction, il se peut que vous deviez CloudFront corriger des erreurs, telles que des erreurs HTTP 5xx. Les erreurs peuvent être de différents types : une réponse non valide renvoyée par la fonction Lambda, des erreurs d'exécution lorsque la fonction est déclenchée, ou encore des erreurs en raison de la limitation d'exécution par le service Lambda. Les sections de cette rubrique donnent des stratégies pour déterminer le type de défaillance qui est à l'origine du problème, puis les étapes à suivre afin de résoudre le problème.

> **Note**
>
> Lorsque vous consultez des fichiers CloudWatch journaux ou des indicateurs pour résoudre des erreurs, sachez qu'ils sont affichés ou stockés à l'emplacement le Région AWS plus

proche de l'endroit où la fonction s'est exécutée. Ainsi, si vous avez un site Web ou une application Web avec des utilisateurs au Royaume-Uni, et qu'une fonction Lambda est associée à votre distribution, par exemple, vous devez modifier la région pour afficher les métriques ou CloudWatch les fichiers journaux de Londres. Région AWS Pour plus d'informations, consultez the section called “Définition de la région Lambda@Edge”.

Rubriques

- Test de vos fonctions Lambda@Edge
- Identifiez les erreurs de fonction Lambda @Edge dans CloudFront
- Dépannage en cas de réponses de fonction Lambda@Edge non valide (erreurs de validation)
- Dépannage des erreurs d'exécution de fonction Lambda@Edge
- Définition de la région Lambda@Edge
- Déterminez si votre compte envoie les journaux vers CloudWatch

Test de vos fonctions Lambda@Edge

Il existe deux étapes pour tester votre fonction Lambda : le test autonome et le test d'intégration.

Test de la fonctionnalité autonome

Avant d'ajouter votre fonction Lambda à CloudFront, assurez-vous de la tester d'abord en utilisant les fonctionnalités de test de la console Lambda ou en utilisant d'autres méthodes. Pour plus d'informations sur les tests de la console Lambda, consultez Invoquer une fonction Lambda avec la console dans le Guide du développeur AWS Lambda .

Testez le fonctionnement de votre fonction dans CloudFront

Il est important de réaliser des tests d'intégration, dans lesquels votre fonction est associée à une distribution et s'exécute en fonction d'un CloudFront événement. Assurez-vous que la fonction est déclenchée pour le bon événement, et qu'elle renvoie une réponse valide et correcte CloudFront. Par exemple, assurez-vous que la structure de l'événement est correcte, que seuls les en-têtes valides sont inclus, etc.

Au fur et à mesure que vous testez l'intégration de votre fonction dans la console Lambda, reportez-vous aux étapes du didacticiel Lambda @Edge pour modifier votre code ou CloudFront le déclencheur qui appelle votre fonction. Par exemple, vérifiez que vous travaillez avec une

version numérotée de votre fonction, comme le décrit cette étape du tutoriel : Étape 4 : ajouter un CloudFront déclencheur pour exécuter la fonction.

Lorsque vous apportez des modifications et que vous les déployez, sachez qu'il faudra plusieurs minutes pour que votre fonction et vos CloudFront déclencheurs mis à jour soient répliqués dans toutes les régions. Cela prend généralement quelques minutes, mais peut durer jusqu'à 15 minutes.

Vous pouvez vérifier si la réplication est terminée en accédant à la CloudFront console et en consultant votre distribution.

Pour vérifier si le déploiement de votre réplication est terminé

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez le nom de la distribution.
3. Vérifiez que le statut de distribution passe de En cours à Déployé, ce qui signifie que votre fonction a été répliquée. Suivez les étapes de la section suivante afin de vérifier que la fonction s'exécute correctement.

Sachez que les tests effectués dans la console valident uniquement la logique de votre fonction et n'appliquent pas de quotas (auparavant appelés limites) de service spécifiques à Lambda@Edge.

Identifiez les erreurs de fonction Lambda @Edge dans CloudFront

Une fois que vous avez vérifié que la logique de votre fonction fonctionne correctement, des erreurs HTTP 5xx peuvent encore s'afficher lors de l'exécution de votre fonction. CloudFront Les erreurs HTTP 5xx peuvent être renvoyées pour diverses raisons, notamment des erreurs liées à la fonction Lambda ou d'autres problèmes. CloudFront

- Si vous utilisez les fonctions Lambda @Edge, vous pouvez utiliser les graphiques de la CloudFront console pour identifier la cause de l'erreur, puis essayer de la corriger. Par exemple, vous pouvez voir si les erreurs HTTP 5xx sont causées par CloudFront ou par des fonctions Lambda, puis, pour des fonctions spécifiques, vous pouvez consulter les fichiers journaux associés afin d'étudier le problème.

- Pour résoudre les erreurs HTTP en général dans CloudFront, consultez les étapes de résolution des problèmes décrites dans la rubrique suivante :Résolution des problèmes liés aux codes d'état de réponse aux erreurs dans CloudFront.

Quelles sont les causes des erreurs de fonction Lambda @Edge dans CloudFront

Il existe plusieurs raisons pour lesquelles une fonction Lambda peut entraîner une erreur HTTP 5xx. Les étapes de résolution à suivre dépendent du type d'erreur. Les erreurs peuvent être classées comme suit :

Une erreur d'exécution de la fonction Lambda

> Une erreur d'exécution se produit lorsque Lambda CloudFront ne reçoit pas de réponse en raison d'exceptions non gérées dans la fonction ou d'une erreur dans le code. Par exemple, si le code comprend le rappel (Error).

Une réponse de fonction Lambda non valide est renvoyée à CloudFront

> Une fois la fonction exécutée, CloudFront reçoit une réponse de Lambda. Une erreur est renvoyée si la structure d'objet de la réponse n'est pas conforme à Structure d'événement Lambda@Edge ou si la réponse contient des en-têtes ou d'autres champs non valides.

L'exécution dans CloudFront est limitée en raison des quotas de service Lambda (anciennement appelés limites)

> Le service Lambda limite les exécutions dans chaque région, et renvoie une erreur si vous dépassez le quota. Pour plus d’informations, consultez Quotas sur Lambda@Edge.

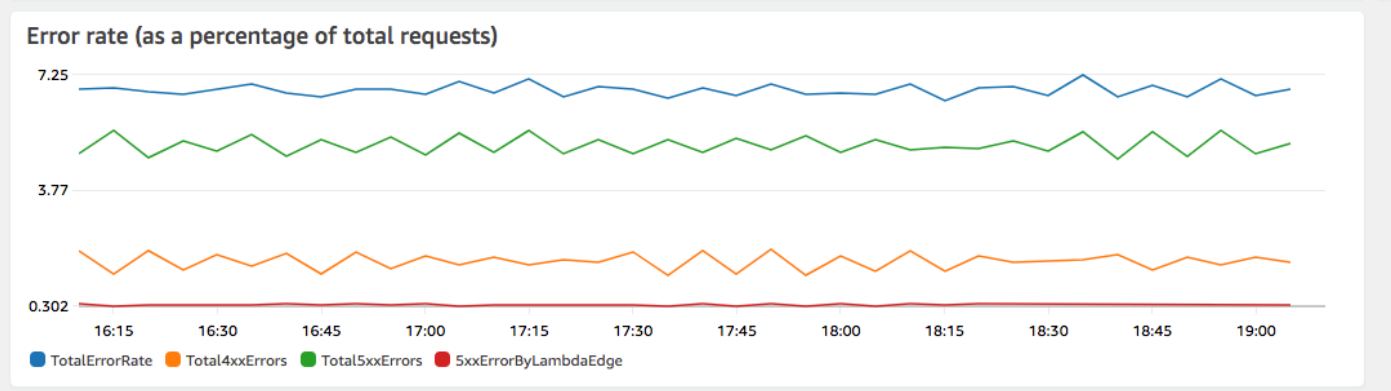
Comment déterminer le type d'échec

Pour vous aider à décider sur quoi vous concentrer lorsque vous débugez et que vous vous efforcez de résoudre les erreurs renvoyées CloudFront, il est utile de déterminer pourquoi une erreur HTTP CloudFront est renvoyée. Pour commencer, vous pouvez utiliser les graphiques fournis dans la section Surveillance de la CloudFront console sur le Console de gestion AWS. Pour plus d'informations sur l'affichage des graphiques dans la section Surveillance de la CloudFront console, consultezSurveillez CloudFront les métriques avec Amazon CloudWatch.

Les graphiques suivants peuvent être particulièrement utiles lorsque vous souhaitez retracer si des erreurs sont renvoyées par les origines ou par une fonction Lambda, et pour réduire le type de problème lorsqu'il s'agit d'une erreur provenant d'une fonction Lambda.

Graphique des taux d'erreurs

L'un des graphiques que vous pouvez afficher dans l'onglet Présentation pour chacune de vos distributions est un graphique de taux d'erreurs. Ce graphique affiche le taux d'erreurs sous forme de pourcentage du nombre total de demandes adressées à votre distribution. Ce graphique montre le taux d'erreurs total, le total des erreurs 4xx, le total des erreurs 5xx et le total des erreurs 5xx provenant des fonctions Lambda. Selon le type d'erreur et le volume, vous pouvez prendre des mesures pour étudier et résoudre le problème initial.



- Si vous voyez des erreurs Lambda, vous pouvez poursuivre vos investigations en examinant les types d'erreurs spécifiques que la fonction renvoie. L'onglet Lambda@Edge errors (Erreurs Lambda@Edge) inclut des graphiques qui classent les erreurs de fonction par type pour vous aider à identifier le problème pour une fonction spécifique.
- Si vous CloudFront constatez des erreurs, vous pouvez les résoudre et vous efforcer de corriger les erreurs d'origine ou de modifier votre CloudFront configuration. Pour plus d'informations, consultez Résolution des problèmes liés aux codes d'état de réponse aux erreurs dans CloudFront.

Graphiques des erreurs d'exécution et des réponses de fonction non valide

L'onglet Lambda@Edge errors (Erreurs Lambda@Edge) inclut des graphiques permettant de classer les erreurs Lambda@Edge pour une distribution spécifique, par type. Par exemple, un graphique montre toutes les erreurs d'exécution par Région AWS.

Pour faciliter la résolution des problèmes, vous pouvez rechercher des problèmes spécifiques en ouvrant et en examinant les fichiers journaux des fonctions spécifiques par région.

Pour afficher les fichiers journaux d'une fonction spécifique par région

1. Dans l'onglet Erreurs Lambda@Edge, sous Fonctions Lambda@Edge associées, choisissez le nom de la fonction, puis choisissez Afficher les métriques.

2. Ensuite, sur la page affichant le nom de votre fonction, dans le coin supérieur droit, choisissez Afficher les journaux de fonction, puis sélectionnez une Région.

   Par exemple, si vous constatez des problèmes dans le graphique Erreurs pour la Région USA Ouest (Oregon), choisissez cette Région dans la liste déroulante. Cela ouvre la CloudWatch console Amazon.

3. Dans la CloudWatch console de cette région, sous Log streams, choisissez un log stream pour afficher les événements liés à la fonction.

De plus, lisez les sections suivantes de ce chapitre pour plus de recommandations sur le dépannage et la correction des erreurs.

Graphique des limitations

L'onglet Lambda@Edge errors (Erreurs Lambda@Edge) inclut également un graphique Throttles (Limitations). Occasionnellement, le service Lambda limite vos appels de fonction par région si vous atteignez le quota (auparavant appelé limite) de simultanéité régionale. Si vous voyez une erreur de dépassement de limite, cela signifie que votre fonction a atteint un quota que le service Lambda impose sur les exécutions dans une région. Pour obtenir plus d'informations sur ces limites et découvrir comment demander une augmentation du quota, consultez Quotas sur Lambda@Edge.



Pour obtenir un exemple sur la façon d'utiliser ces informations pour résoudre des erreurs HTTP, consultez le billet de blog Four steps for debugging your content delivery on AWS.

Dépannage en cas de réponses de fonction Lambda@Edge non valide (erreurs de validation)

Si vous identifiez que votre problème est dû à une erreur de validation Lambda, cela signifie que votre fonction Lambda renvoie une réponse non valide à. CloudFront Suivez les instructions de cette section pour prendre les mesures nécessaires pour revoir votre fonction et vous assurer que votre réponse est conforme aux CloudFront exigences.

CloudFront valide la réponse d'une fonction Lambda de deux manières :

- La réponse Lambda doit se conformer à la structure d'objet requise. Voici des exemples de mauvaise structure d'objet : impossible d'analyser JSON, champs obligatoires manquants et la réponse contient un objet non valide. Pour plus d'informations, consultez Structure d'événement Lambda@Edge.
- La réponse doit inclure uniquement les valeurs d'objet valides. Une erreur se produit si la réponse inclut un objet valide mais dont les valeurs ne sont pas prises en charge. Les exemples incluent les éléments suivants : ajout ou mise à jour d'en-têtes non autorisés ou en lecture seule (voir Restrictions sur les fonctions périphériques), dépassement des limitations de taille du corps (voir Limites sur la taille de la réponse générée dans la rubrique Lambda@Edge Erreurs) et les caractères ou les valeurs non valables (voir Structure d'événement Lambda@Edge).

Lorsque Lambda renvoie une réponse non valide à CloudFront, des messages d'erreur sont écrits CloudWatch dans des fichiers journaux qui sont CloudFront redirigés vers la région où la fonction Lambda a été exécutée. C'est le comportement par défaut auquel les fichiers journaux sont envoyés en CloudWatch cas de réponse non valide. Toutefois, si vous avez associé une fonction Lambda à une fonction Lambda CloudFront avant son lancement, il est possible qu'elle ne soit pas activée pour votre fonction. Pour plus d'informations, consultez la section Déterminez si votre compte transmet les fichiers journaux à CloudWatch plus loin dans la rubrique.

CloudFront envoie les fichiers journaux vers la région correspondant à l'endroit où votre fonction a été exécutée, dans le groupe de journaux associé à votre distribution. Les groupes de journaux ont le format suivant :`/aws/cloudfront/LambdaEdge/`*`DistributionId`*, où *`DistributionId`* est l'ID de votre distribution. Pour déterminer la région dans laquelle se trouvent les fichiers CloudWatch journaux, consultez la section Détermination de la région Lambda @Edge plus loin dans cette rubrique.

Si l'erreur est reproductible, vous pouvez créer une nouvelle demande qui entraîne l'erreur, puis rechercher l'identifiant de la demande dans une CloudFront réponse ayant échoué (`X-Amz-Cf-`

Iden-tête) afin de localiser un seul échec dans les fichiers journaux. L'entrée du fichier journal inclut des informations susceptibles de vous aider à identifier les raisons pour lesquelles l'erreur est renvoyée, et affiche aussi l'ID de demande Lambda correspondant, ce qui vous permet d'analyser la cause première dans le cadre d'une seule demande.

Si une erreur est intermittente, vous pouvez utiliser les journaux d' CloudFront accès pour trouver l'identifiant d'une demande qui a échoué, puis rechercher dans CloudWatch les journaux les messages d'erreur correspondants. Pour plus d'informations, consultez la section précédente, Détermination du type d'échec.

Dépannage des erreurs d’exécution de fonction Lambda@Edge

Si le problème provient d'une erreur d'exécution Lambda, il peut être utile de créer des instructions de journalisation pour les fonctions Lambda, d'écrire des messages dans des fichiers CloudWatch journaux qui surveillent l'exécution de votre fonction CloudFront et déterminent si elle fonctionne comme prévu. Vous pouvez ensuite rechercher ces instructions dans les fichiers CloudWatch journaux pour vérifier que votre fonction fonctionne.

> **Note**
>
> Même si vous n'avez pas modifié votre fonction Lambda@Edge, les mises à jour de l'environnement d'exécution de la fonction Lambda peuvent l'affecter et renvoyer une erreur d'exécution. Pour plus d'informations sur les tests et la migration vers une version ultérieure, consultez Prochaines mises à jour de l'environnement d'exécution AWS Lambda et AWS Lambda @Edge.

Définition de la région Lambda@Edge

Pour connaître les régions dans lesquelles votre fonction Lambda @Edge reçoit du trafic, consultez les métriques de la fonction sur la CloudFront console du. Console de gestion AWS Les statistiques sont affichées pour chaque AWS région. Sur la même page, vous pouvez choisir une région et afficher les fichiers journaux pour cette région afin de pouvoir rechercher des problèmes. Vous devez consulter les fichiers CloudWatch journaux dans la AWS région appropriée pour voir les fichiers journaux créés lors de l' CloudFront exécution de votre fonction Lambda.

Pour plus d'informations sur l'affichage des graphiques dans la section Surveillance de la CloudFront console, consultezSurveillez CloudFront les métriques avec Amazon CloudWatch.

Déterminez si votre compte envoie les journaux vers CloudWatch

Par défaut, CloudFront active la journalisation des réponses de la fonction Lambda non valides et envoie les fichiers journaux vers CloudWatch . Service-linked rôles pour Lambda @Edge Si vous avez ajouté des fonctions Lambda @Edge CloudFront avant la publication de la fonctionnalité de journal des réponses des fonctions Lambda non valide, la journalisation est activée lors de la prochaine mise à jour de votre configuration Lambda @Edge, par exemple en ajoutant un déclencheur. CloudFront

Vous pouvez vérifier que le transfert des fichiers journaux vers CloudWatch est activé pour votre compte en procédant comme suit :

- Vérifiez si les journaux apparaissent dans CloudWatch — Assurez-vous de regarder dans la région où la fonction Lambda @Edge s'est exécutée. Pour plus d'informations, consultez Définition de la région Lambda@Edge.
- Déterminez si le rôle lié au service associé existe dans votre compte IAM : vous devez disposer du rôle IAM `AWSServiceRoleForCloudFrontLogger` dans votre compte. Pour plus d'informations sur ce rôle, consultez Service-linked rôles pour Lambda @Edge.

Suppression des fonctions et des réplicas Lambda@Edge

Vous pouvez supprimer une fonction Lambda@Edge uniquement lorsque les réplicas de cette fonction ont été supprimés par CloudFront. Les réplicas d'une fonction Lambda sont automatiquement supprimés dans les cas suivants :

- Après avoir supprimé la dernière association de la fonction de toutes vos distributions CloudFront. Si plusieurs distributions utilisent une fonction, les réplicas ne sont supprimés qu'après avoir supprimé l'association de fonctions de la dernière distribution.
- Après avoir supprimé la dernière distribution à laquelle une fonction était associée.

Ils sont généralement supprimés en quelques heures. Vous ne pouvez pas supprimer manuellement des réplicas de fonction Lambda@Edge. Cela permet d'éviter la suppression d'un réplica en cours d'utilisation, ce qui entraînerait une erreur.

> **Warning**
>
> Ne créez pas d'applications qui utilisent des répliques de fonctions Lambda @Edge en dehors de. CloudFront Ces réplicas sont supprimés lorsque leurs associations avec des distributions sont supprimées, ou lorsque les distributions elles-mêmes sont supprimées. Le réplica dont dépend une application externe pourrait être supprimé sans avertissement, ce qui entraînerait un échec.

Pour supprimer une association de fonctions Lambda @Edge d'une distribution CloudFront

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez l'ID de la distribution qui possède l'association de la fonction Lambda@Edge que vous souhaitez supprimer.
3. Choisissez l'onglet Comportements.
4. Sélectionnez le comportement de cache qui contient l'association à la fonction Lambda@Edge que vous souhaitez supprimer, puis choisissez Modifier.
5. Sous Associations de fonctions, Type de fonction, choisissez Aucune association pour supprimer l'association de fonctions Lambda@Edge.
6. Cliquez sur Enregistrer les modifications.

Après avoir supprimé une association de fonctions Lambda @Edge d'une CloudFront distribution, vous pouvez éventuellement supprimer la fonction Lambda ou la version de la fonction de. AWS Lambda Patientez quelques heures après avoir supprimé l'association de la fonction pour permettre le nettoyage des réplicas de la fonction Lambda@Edge. Ensuite, vous pouvez supprimer la fonction à l'aide de la console Lambda, de l'API AWS CLI Lambda ou d'un SDK. AWS

Vous pouvez également supprimer une version spécifique d'une fonction Lambda si aucune CloudFront distribution n'est associée à cette version. Une fois toutes les associations supprimées pour une version de fonction Lambda, patientez quelques heures. Vous pourrez alors supprimer la version de la fonction.

Structure d'événement Lambda@Edge

Les rubriques suivantes décrivent les objets d'événements de demande et de réponse CloudFront transmis à une fonction Lambda @Edge lorsqu'elle est déclenchée.

Rubriques

- Sélection de l'origine dynamique
- Événements de demande
- Événements de réponse

Sélection de l'origine dynamique

Vous pouvez utiliser le modèle de chemin dans un comportement de cache pour router les demandes vers une origine, en fonction du chemin et du nom de l'objet demandé, tels que `images/*.jpg`. En utilisant Lambda@Edge, vous pouvez également acheminer des demandes vers une origine en fonction d'autres caractéristiques, comme les valeurs contenues dans les en-têtes de la demande.

Cette sélection d'origine dynamique peut être utile de diverses façons. Par exemple, vous pouvez répartir les demandes entre des origines de différentes zones géographiques pour vous aider à réaliser un équilibrage de charge international. Ou vous pouvez acheminer de façon sélective des demandes vers différentes origines servant chacune une fonction donnée : gestion du robot, optimisation de la stratégie SEO, authentification, etc. Pour obtenir des exemples de code qui expliquent comment utiliser cette fonctionnalité, consultez Content-based sélection dynamique de l'origine - exemples.

Dans l'événement de demande CloudFront d'origine, l'`origin`objet de la structure d'événement contient des informations sur l'origine vers laquelle la demande serait acheminée, en fonction du modèle de chemin. Vous pouvez mettre à jour les valeurs de l'objet `origin` pour router une demande vers une autre origine. Quand vous mettez à jour l'objet `origin`, vous n'avez pas besoin de définir l'origine dans la distribution. Vous pouvez également remplacer un objet d'origine Amazon S3 par un objet d'origine personnalisée, et vice versa. Toutefois, vous ne pouvez spécifier qu'une seule origine par demande ; une origine personnalisée ou une origine Amazon S3, mais pas les deux.

Événements de demande

Les rubriques suivantes présentent la structure de l'objet qui est transmis à CloudFront une fonction Lambda pour les événements de demande d'affichage et d'origine. Ces exemples montrent une demande `GET` sans corps. Après les exemples, vous trouverez la liste de tous les champs possibles dans les événements de demande d'utilisateur et d'origine.

Rubriques

- Exemple de demande d'utilisateur
- Exemple de demande de l'origine
- Champs d'événement de demande

Exemple de demande d'utilisateur

L'exemple suivant montre un objet d'événement de demande d'utilisateur.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "viewer-request",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "host": [
              {
                "key": "Host",
                "value": "d111111abcdef8.cloudfront.net"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "curl/7.66.0"
              }
            ],
            "accept": [
              {
                "key": "accept",
                "value": "*/*"
              }
            ]
          },
          "method": "GET",
          "querystring": "",
```

```
          "uri": "/"
        }
      }
    }
  ]
}
```

Exemple de demande de l'origine

L'exemple suivant montre un objet d'événement de demande d'origine.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "origin-request",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "x-forwarded-for": [
              {
                "key": "X-Forwarded-For",
                "value": "203.0.113.178"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "Amazon CloudFront"
              }
            ],
            "via": [
              {
                "key": "Via",
                "value": "2.0 2afae0d44e2540f472c0635ab62c232b.cloudfront.net
 (CloudFront)"
              }
            ],
            "host": [
```

```
            {
              "key": "Host",
              "value": "example.org"
            }
          ],
          "cache-control": [
            {
              "key": "Cache-Control",
              "value": "no-cache"
            }
          ]
        },
        "method": "GET",
        "origin": {
          "custom": {
            "customHeaders": {},
            "domainName": "example.org",
            "keepaliveTimeout": 5,
            "path": "",
            "port": 443,
            "protocol": "https",
            "readTimeout": 30,
            "responseCompletionTimeout": 30,
            "sslProtocols": [
              "TLSv1",
              "TLSv1.1",
              "TLSv1.2"
            ]
          }
        },
        "querystring": "",
        "uri": "/"
      }
    }
  ]
}
```

Champs d'événement de demande

Les données d'objet d'événement de demande sont contenues dans deux sous-objets : `config` (`Records.cf.config`) et `request` (`Records.cf.request`). Les listes suivantes décrivent les champs de chaque sous-objet.

Champs de l’objet config

La liste suivante décrit les champs figurant dans l’objet `config` (`Records.cf.config`).

`distributionDomainName` (lecture seule)

Nom de domaine de la distribution qui est associée à la demande.

`distributionID` (lecture seule)

ID de la distribution qui est associée à la demande.

`eventType` (lecture seule)

Type de déclencheur associé à la demande : `viewer-request` ou `origin-request`.

`requestId` (lecture seule)

Chaîne chiffrée qui identifie de façon unique une demande de l'utilisateur à CloudFront. La valeur `requestId` apparaît également dans les journaux d'accès de CloudFront en tant que `x-edge-request-id`. Pour plus d’informations, consultez Journaux d'accès (journaux standard) et Champs du fichier journal.

Champs de l'objet de demande

La liste suivante décrit les champs figurant dans l’objet `request` (`Records.cf.request`).

`clientIp` (lecture seule)

Adresse IP de l'utilisateur qui a émis la requête. Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur correspond à l'adresse IP du proxy ou de l'équilibreur de charge.

en-têtes () read/write

En-têtes de la requête. Remarques :

- Les clés figurant dans l’objet `headers` sont les versions en minuscules des noms d’en-têtes HTTP standard. L'utilisation des minuscules vous permet d'accéder aux valeurs des en-têtes sans tenir compte de la casse.
- Chaque objet d’en-tête (par exemple, `headers["accept"]` ou `headers["host"]`) est un tableau de paires clé-valeur. Pour un en-tête donné, le tableau contient une paire clé-valeur pour chaque valeur dans la demande.

- `key` contient le nom sensible à la casse de l'en-tête tel qu'il apparaissait dans la demande HTTP ; par exemple, `Host`, `User-Agent`, `X-Forwarded-For`, `Cookie`, etc.
- `value` contient la valeur d'en-tête telle qu'elle apparaissait dans la requête HTTP.
- Lorsque votre fonction Lambda ajoute ou modifie des en-têtes de demande et que vous n'incluez pas le champ `key` d'en-tête, Lambda@Edge insère automatiquement une clé (`key`) d'en-tête en utilisant le nom d'en-tête que vous fournissez. Quelle que soit la manière dont vous avez formaté le nom d'en-tête, la clé d'en-tête qui est insérée automatiquement est formatée avec une majuscule initiale pour chaque partie, séparée par des tirets (-).

  Par exemple, vous pouvez ajouter un en-tête comme le suivant, sans clé (`key`) d'en-tête :

  ```
  "user-agent": [
    {
      "value": "ExampleCustomUserAgent/1.X.0"
    }
  ]
  ```

  Dans cet exemple, Lambda@Edge insère automatiquement `"key": "User-Agent"`.

Pour plus d'informations sur les restrictions applicables à l'utilisation d'en-têtes, consultez Restrictions sur les fonctions périphériques.

`method` (lecture seule)

Méthode HTTP de la demande.

`querystring` (read/write)

Chaîne de requête, le cas échéant, dans la demande. Si la demande n'inclut pas de chaîne de requête, l'objet d'événement inclut quand-même `querystring` avec une valeur vide. Pour plus d'informations sur les chaînes de requête, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête.

`uri` (read/write)

Chemin d'accès relatif de l'objet demandé. Si votre fonction Lambda modifie la valeur `uri`, notez ce qui suit :

- La nouvelle valeur `uri` doit commencer par une barre oblique (/).
- Lorsqu'une fonction modifie la valeur `uri`, cela change l'objet que l'utilisateur demande.
- Lorsqu'une fonction modifie la valeur `uri`, cela ne modifie pas le comportement de cache pour la demande ou l'origine vers laquelle la demande est envoyée.

`body` (read/write)

Corps de la requête HTTP. La structure `body` peut contenir les champs suivants :

`inputTruncated` (lecture seule)

Indicateur booléen qui indique si le corps a été tronqué par Lambda@Edge. Pour plus d'informations, consultez Restrictions relatives au corps de la requête avec l'option Inclure le corps.

`action` (read/write)

L'action que vous avez l'intention de prendre avec le corps. Les options pour l'`action`sont les suivantes :

- `read-only:` Il s'agit de l'option par défaut. Au moment de renvoyer la réponse à partir de la fonction Lambda, si `action` est en lecture seule, Lambda@Edge ignore les modifications apportée à `encoding` ou à `data`.
- `replace:` À préciser lorsque vous souhaitez remplacer le corps envoyé à l'origine.

`encoding` (read/write)

L'encodage pour le corps. Lorsque Lambda@Edge expose le corps à la fonction Lambda, il convertit d'abord le corps en base64-encoding. Si vous choisissez `replace` comme `action` pour remplacer le corps, vous pouvez choisir d'utiliser l'encodage `base64` (option par défaut) ou `text`. Si vous précisez `encoding` comme `base64`, mais que le corps n'est pas valide base64, CloudFront renvoie une erreur.

`data` (read/write)

Le contenu du corps de requête.

`origin`(read/write) (événements d'origine uniquement)

Origine vers laquelle envoyer la demande. La structure `origin` doit contenir une unique origine, qui peut être une origine personnalisée ou une origine Amazon S3.

Selon le type d'origine que vous spécifiez (origine personnalisée ou origine Amazon S3), vous devez indiquer les champs suivants dans votre demande :

`customHeaders`(read/write) (personnalisé et origines d'Amazon S3)

(Facultatif) Vous pouvez inclure des en-têtes personnalisés dans la demande en spécifiant un nom et une valeur d'en-tête pour chacun d'eux. Vous ne pouvez pas ajouter des en-têtes non autorisés et un en-tête portant le même nom ne peut pas être présent dans

`Records.cf.request.headers`. Les notes sur les en-têtes de demande s'appliquent également aux en-têtes personnalisés. Pour plus d'informations, consultez En-têtes personnalisés qui ne CloudFront peuvent pas être ajoutés aux demandes d'origine et Restrictions sur les fonctions périphériques.

`domainName`(read/write) (personnalisé et origines d'Amazon S3)

Nom de domaine de l'origine. Le nom de domaine ne peut pas être vide.

- Pour les origines personnalisées – Spécifiez un nom de domaine DNS, tel que `www.example.com`. Le nom de domaine ne peut pas inclure un signe deux-points (:) et ne peut pas être une adresse IP. Le nom du domaine peut contenir jusqu'à 253 caractères.
- Pour les origines Amazon S3 – Spécifiez le nom de domaine DNS du compartiment Amazon S3, tel que `amzn-s3-demo-bucket.s3.eu-west-1.amazonaws.com`. Il peut comporter jusqu'à 128 caractères, qui doivent tous être en minuscules.

`path`(read/write) (personnalisé et origines d'Amazon S3)

Chemin de répertoire à l'origine où la demande doit localiser le contenu. Ce chemin doit commencer par une barre oblique (/) mais ne doit pas se terminer par une barre oblique (par exemple, il ne doit pas se terminer par `example-path/`). Pour les origines personnalisées uniquement, le chemin doit être codé par URL et avoir une longueur maximale de 255 caractères.

`keepaliveTimeout`(read/write) (origines personnalisées uniquement)

Combien de temps, en secondes, cela CloudFront devrait essayer de maintenir la connexion à l'origine après avoir reçu le dernier paquet de la réponse. La valeur doit être un nombre compris entre 1 et 120 inclus.

`port`(read/write) (origines personnalisées uniquement)

Le port auquel vous CloudFront devez vous connecter à votre point d'origine personnalisé. Il doit s'agir du port 80, du port 443 ou d'un port compris entre 1 024 et 65 535.

`protocol`(read/write) (origines personnalisées uniquement)

Le protocole de connexion à utiliser CloudFront lors de la connexion à votre point d'origine. La valeur peut être `http` ou `https`.

`readTimeout`(read/write) (personnalisé et origines d'Amazon S3)

Combien de temps, en secondes, CloudFront doit attendre une réponse après avoir envoyé une demande à votre origine. Cela spécifie également la durée pendant laquelle CloudFront

doit attendre après avoir reçu un paquet d'une réponse et avant de recevoir le paquet suivant. La valeur doit être un nombre compris entre 1 et 120 inclus.

Si vous avez besoin d'un quota plus élevé, consultez Délai de réponse par origine.

`responseCompletionTimeout`(read/write) (personnalisé et origines d'Amazon S3)

Durée (en secondes) pendant laquelle une demande provenant CloudFront de l'origine peut rester ouverte et attendre une réponse. Si la réponse complète n'est pas reçue de l'origine à ce moment-là, CloudFront met fin à la connexion.

La valeur de `responseCompletionTimeout` doit être supérieure ou égale à la valeur de `readTimeout`. En définissant cette valeur sur 0, vous effacez toute valeur précédemment définie et rétablissez la valeur par défaut. Vous pouvez également obtenir le même résultat en supprimant le champ `responseCompletionTimeout` de la demande d'événement.

`sslProtocols`(read/write) (origines personnalisées uniquement)

SSL/TLS Protocole minimal à CloudFront utiliser lors de l'établissement d'une connexion HTTPS avec votre point d'origine. Il peut s'agir des valeurs suivantes : `TLSv1.2`, `TLSv1.1`, `TLSv1` ou `SSLv3`.

`authMethod`(read/write) (Origines Amazon S3 uniquement)

Si vous utilisez une identité d'accès à l'origine (OAI), définissez ce champ sur `origin-access-identity`. Si vous n'utilisez pas d'OAI, configurez-le sur `none`. Si vous définissez `authMethod` sur `origin-access-identity`, il existe plusieurs exigences :

- Vous devez spécifier le paramètre `region` (voir le champ suivant).
- Vous devez utiliser la même identité d'accès à l'origine lorsque vous changez l'origine Amazon S3 de la demande.
- Vous ne pouvez pas utiliser d'identité d'accès à l'origine lorsque vous remplacez l'origine personnalisée de la demande par une origine Amazon S3.

> **Note**
>
> Ce champ ne prend pas en charge le contrôle d'accès à l'origine (OAC).

`region`(read/write) (Origines Amazon S3 uniquement)

La AWS région de votre compartiment Amazon S3. Cette option n'est requise que lorsque vous définissez `authMethod` sur `origin-access-identity`.

Événements de réponse

Les rubriques suivantes présentent la structure de l'objet qui est CloudFront transmis à une fonction Lambda pour les événements de réponse du visualiseur et de l'origine. Après les exemples, vous trouverez la liste de tous les champs possibles dans les événements de réponse d'utilisateur et d'origine.

Rubriques

- Exemple de réponse de l'origine
- Exemple de réponse de l'utilisateur
- Champs d'événement de réponse

Exemple de réponse de l'origine

L'exemple suivant montre un objet d'événement de réponse de l'origine.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "origin-response",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "x-forwarded-for": [
              {
                "key": "X-Forwarded-For",
                "value": "203.0.113.178"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "Amazon CloudFront"
              }
            ],
```

```
            "via": [
              {
                "key": "Via",
                "value": "2.0 8f22423015641505b8c857a37450d6c0.cloudfront.net
 (CloudFront)"
              }
            ],
            "host": [
              {
                "key": "Host",
                "value": "example.org"
              }
            ],
            "cache-control": [
              {
                "key": "Cache-Control",
                "value": "no-cache"
              }
            ]
          },
          "method": "GET",
          "origin": {
            "custom": {
              "customHeaders": {},
              "domainName": "example.org",
              "keepaliveTimeout": 5,
              "path": "",
              "port": 443,
              "protocol": "https",
              "readTimeout": 30,
              "responseCompletionTimeout": 30,
              "sslProtocols": [
                "TLSv1",
                "TLSv1.1",
                "TLSv1.2"
              ]
            }
          },
          "querystring": "",
          "uri": "/"
        },
        "response": {
          "headers": {
            "access-control-allow-credentials": [
```

```
            {
              "key": "Access-Control-Allow-Credentials",
              "value": "true"
            }
          ],
          "access-control-allow-origin": [
            {
              "key": "Access-Control-Allow-Origin",
              "value": "*"
            }
          ],
          "date": [
            {
              "key": "Date",
              "value": "Mon, 13 Jan 2020 20:12:38 GMT"
            }
          ],
          "referrer-policy": [
            {
              "key": "Referrer-Policy",
              "value": "no-referrer-when-downgrade"
            }
          ],
          "server": [
            {
              "key": "Server",
              "value": "ExampleCustomOriginServer"
            }
          ],
          "x-content-type-options": [
            {
              "key": "X-Content-Type-Options",
              "value": "nosniff"
            }
          ],
          "x-frame-options": [
            {
              "key": "X-Frame-Options",
              "value": "DENY"
            }
          ],
          "x-xss-protection": [
            {
              "key": "X-XSS-Protection",
```

```
                "value": "1; mode=block"
              }
            ],
            "content-type": [
              {
                "key": "Content-Type",
                "value": "text/html; charset=utf-8"
              }
            ],
            "content-length": [
              {
                "key": "Content-Length",
                "value": "9593"
              }
            ]
          },
          "status": "200",
          "statusDescription": "OK"
        }
      }
    }
  ]
}
```

Exemple de réponse de l'utilisateur

L'exemple suivant montre un objet d'événement de réponse de l'utilisateur.

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionDomainName": "d111111abcdef8.cloudfront.net",
          "distributionId": "EDFDVBD6EXAMPLE",
          "eventType": "viewer-response",
          "requestId": "4TyzHTaYWb1GX1qTfsHhEqV6HUDd_BzoBZnwfnvQc_1oF26ClkoUSEQ=="
        },
        "request": {
          "clientIp": "203.0.113.178",
          "headers": {
            "host": [
              {
                "key": "Host",
```

```
            "value": "d111111abcdef8.cloudfront.net"
          }
        ],
        "user-agent": [
          {
            "key": "User-Agent",
            "value": "curl/7.66.0"
          }
        ],
        "accept": [
          {
            "key": "accept",
            "value": "*/*"
          }
        ]
      },
      "method": "GET",
      "querystring": "",
      "uri": "/"
    },
    "response": {
      "headers": {
        "access-control-allow-credentials": [
          {
            "key": "Access-Control-Allow-Credentials",
            "value": "true"
          }
        ],
        "access-control-allow-origin": [
          {
            "key": "Access-Control-Allow-Origin",
            "value": "*"
          }
        ],
        "date": [
          {
            "key": "Date",
            "value": "Mon, 13 Jan 2020 20:14:56 GMT"
          }
        ],
        "referrer-policy": [
          {
            "key": "Referrer-Policy",
            "value": "no-referrer-when-downgrade"
```

```
            }
          ],
          "server": [
            {
              "key": "Server",
              "value": "ExampleCustomOriginServer"
            }
          ],
          "x-content-type-options": [
            {
              "key": "X-Content-Type-Options",
              "value": "nosniff"
            }
          ],
          "x-frame-options": [
            {
              "key": "X-Frame-Options",
              "value": "DENY"
            }
          ],
          "x-xss-protection": [
            {
              "key": "X-XSS-Protection",
              "value": "1; mode=block"
            }
          ],
          "age": [
            {
              "key": "Age",
              "value": "2402"
            }
          ],
          "content-type": [
            {
              "key": "Content-Type",
              "value": "text/html; charset=utf-8"
            }
          ],
          "content-length": [
            {
              "key": "Content-Length",
              "value": "9593"
            }
          ]
```

```
          },
          "status": "200",
          "statusDescription": "OK"
        }
      }
    }
  ]
}
```

Champs d'événement de réponse

Les données d'objet d'événement de réponse sont contenues dans trois sous-objets : `config` (`Records.cf.config`), `request` (`Records.cf.request`) et `response` (`Records.cf.response`). Pour plus d'informations sur les champs de l'objet de demande, consultez Champs de l'objet de demande. Les listes suivantes décrivent les champs figurant dans les sous-objets `config` et `response`.

Champs de l'objet config

La liste suivante décrit les champs figurant dans l'objet `config` (`Records.cf.config`).

`distributionDomainName` (lecture seule)

Nom de domaine de la distribution qui est associée à la réponse.

`distributionID` (lecture seule)

ID de la distribution qui est associée à la réponse.

`eventType` (lecture seule)

Type de déclencheur associé à la réponse : `origin-response` ou `viewer-response`.

`requestId` (lecture seule)

Chaîne cryptée qui identifie de manière unique le téléspectateur à qui CloudFront cette réponse est associée. La `requestId` valeur apparaît également dans les journaux CloudFront d'accès sous la forme`x-edge-request-id`. Pour plus d'informations, consultez Journaux d'accès (journaux standard) et Champs du fichier journal.

Champs de l'objet de réponse

La liste suivante décrit les champs figurant dans l'objet `response` (`Records.cf.response`). Pour obtenir des informations sur l'utilisation d'une fonction Lambda@Edge pour générer une réponse HTTP, consultez Génération de réponses HTTP dans les déclencheurs de demande.

`headers` (read/write)

En-têtes de la réponse. Remarques :

- Les clés figurant dans l'objet `headers` sont les versions en minuscules des noms d'en-têtes HTTP standard. L'utilisation des minuscules vous permet d'accéder aux valeurs des en-têtes sans tenir compte de la casse.
- Chaque objet d'en-tête (par exemple, `headers["content-type"]` ou `headers["content-length"]`) est un tableau de paires clé-valeur. Pour un en-tête donné, le tableau contient une paire clé-valeur pour chaque valeur de la réponse.
- `key` contient le nom sensible à la casse de l'en-tête tel qu'il apparaît dans la réponse HTTP ; par exemple, `Content-Type`, `Content-Length`, `Cookie`, etc.
- `value` contient la valeur d'en-tête telle qu'elle apparaît dans la réponse HTTP.
- Lorsque votre fonction Lambda ajoute ou modifie des en-têtes de réponse et que vous n'incluez pas le champ `key` d'en-tête, Lambda@Edge insère automatiquement une clé (`key`) d'en-tête en utilisant le nom d'en-tête que vous fournissez. Quelle que soit la manière dont vous avez formaté le nom d'en-tête, la clé d'en-tête qui est insérée automatiquement est formatée avec une majuscule initiale pour chaque partie, séparée par des tirets (-).

  Par exemple, vous pouvez ajouter un en-tête comme le suivant, sans clé (`key`) d'en-tête :

  ```
  "content-type": [
    {
      "value": "text/html;charset=UTF-8"
    }
  ]
  ```

  Dans cet exemple, Lambda@Edge insère automatiquement `"key": "Content-Type"`.

Pour plus d'informations sur les restrictions applicables à l'utilisation d'en-têtes, consultez Restrictions sur les fonctions périphériques.

`status`

Code de statut HTTP de la réponse.

`statusDescription`

Description de l'état HTTP de la réponse.

Utilisation des demandes et des réponses

Pour utiliser les demandes et réponses Lambda@Edge, consultez les rubriques suivantes :

Rubriques

- Utilisation des fonctions Lambda@Edge avec le basculement d'origine
- Génération de réponses HTTP dans les déclencheurs de demande
- Mise à jour des réponses HTTP dans des déclencheurs de réponse de l'origine
- Accès au corps de requête en choisissant l'option Inclure le corps

Utilisation des fonctions Lambda@Edge avec le basculement d'origine

Vous pouvez utiliser les fonctions Lambda @Edge avec des CloudFront distributions que vous avez configurées avec des groupes d'origine, par exemple, pour le basculement d'origine que vous configurez afin de garantir une haute disponibilité. Pour utiliser une fonction Lambda avec un groupe d'origine, spécifiez la fonction dans une requête d'origine ou un déclencheur de réponse de l'origine pour un groupe d'origine lorsque vous créez le comportement de cache.

Pour plus d'informations, consultez les ressources suivantes :

- Création d'un groupe d'origines : Création d'un groupe d'origine
- Comment fonctionne le basculement d'origine avec Lambda@Edge: Utilisation du basculement d'origine avec les fonctions Lambda@Edge

Génération de réponses HTTP dans les déclencheurs de demande

Lorsque CloudFront vous recevez une demande, vous pouvez utiliser une fonction Lambda pour générer une réponse HTTP qui est CloudFront renvoyée directement au visualiseur sans transmettre la réponse à l'origine. La génération de réponses HTTP réduit la charge sur le serveur d'origine, et aussi généralement la latence pour l'utilisateur.

Les scénarios courants pour générer des réponses HTTP sont les suivants :

- Renvoi d'une petite page web à l'utilisateur
- Renvoi d'un code de statut HTTP 301 ou 302 pour rediriger l'utilisateur vers une autre page web
- Renvoi d'un code de statut HTTP 401 lorsque l'utilisateur ne s'est pas authentifié

Une fonction Lambda@Edge peut générer une réponse HTTP lorsque les événements CloudFront suivants se produisent :

Événements de demande utilisateur

Lorsqu'une fonction est déclenchée par un événement de demande du spectateur, CloudFront renvoie la réponse au visualiseur sans la mettre en cache.

Événements de demande à l'origine

Lorsqu'une fonction est déclenchée par un événement de demande d'origine, CloudFront vérifie dans le cache périphérique la présence d'une réponse précédemment générée par la fonction.

- Si la réponse se trouve dans le cache, la fonction n'est pas exécutée et CloudFront renvoie la réponse mise en cache au visualiseur.
- Si la réponse ne se trouve pas dans le cache, la fonction est exécutée et CloudFront retourne la réponse à l'utilisateur et la met dans le cache.

Pour voir un exemple de code permettant de générer des réponses HTTP, consultez Exemples de fonctions Lambda@Edge. Vous pouvez également remplacer les réponses HTTP dans les déclencheurs de réponse. Pour plus d’informations, consultez Mise à jour des réponses HTTP dans des déclencheurs de réponse de l’origine.

Modèle de programmation

Cette section décrit le modèle de programmation permettant d'utiliser Lambda@Edge pour générer des réponses HTTP.

Rubriques

- Objet Réponse
- Erreurs
- Champs obligatoires

Objet Réponse

La réponse que vous renvoyez en tant que paramètre `result` de la méthode `callback` doit avoir la structure suivante (notez que seul le champ `status` est requis).

```
const response = {
    body: 'content',
    bodyEncoding: 'text' | 'base64',
    headers: {
        'header name in lowercase': [{
           key: 'header name in standard case',
           value: 'header value'
         }],
         ...
    },
    status: 'HTTP status code (string)',
    statusDescription: 'status description'
};
```

L'objet de réponse peut inclure les valeurs suivantes :

`body`

Le corps, le cas échéant, que vous CloudFront souhaitez renvoyer dans la réponse générée.

`bodyEncoding`

Encodage de la valeur que vous avez spécifiée dans `body`. Les seuls encodages valides sont `text` et `base64`. Si vous incluez `body` dans l'`response`objet mais que vous l'omettez`bodyEncoding`, CloudFront traite le corps comme du texte.

Si vous spécifiez `bodyEncoding` comme `base64`, mais que le corps n'est pas un base64 valide, CloudFront renvoie une erreur.

`headers`

En-têtes que vous CloudFront souhaitez renvoyer dans la réponse générée. Notez ce qui suit :

- Les clés figurant dans l'objet `headers` sont les versions en minuscules des noms d'en-têtes HTTP standard. L'utilisation des minuscules vous permet d'accéder aux valeurs des en-têtes sans tenir compte de la casse.
- Chaque en-tête (par exemple, `headers["accept"]` ou `headers["host"]`) est un tableau de paires clé-valeur. Pour un en-tête donné, le tableau contient une paire clé-valeur pour chaque valeur de la réponse générée.

- `key` (facultatif) est le nom de l'en-tête sensible à la casse tel qu'il s'affiche dans une demande HTTP, par exemple, `accept` ou `host`.
- Indiquez `value` comme valeur d'en-tête.
- Si vous n'incluez pas la partie clé d'en-tête de la paire clé-valeur, Lambda@Edge insère automatiquement une clé d'en-tête à l'aide du nom d'en-tête que vous fournissez. Quelle que soit la manière dont vous avez formaté le nom d'en-tête, la clé d'en-tête qui est insérée est formatée automatiquement avec une majuscule initiale pour les différentes parties séparées par des tirets (-).

  Par exemple, vous pouvez ajouter un en-tête comme suit, sans clé d'en-tête : `'content-type': [{ value: 'text/html;charset=UTF-8' }]`

  Dans cet exemple, Lambda@Edge crée la clé d'en-tête suivante : `Content-Type`.

Pour plus d'informations sur les restrictions applicables à l'utilisation d'en-têtes, consultez Restrictions sur les fonctions périphériques.

`status`

Le code d'état HTTP . Fournissez le code d'état sous forme de chaîne. CloudFront utilise le code d'état fourni pour les opérations suivantes :

- Renvoi dans la réponse
- Cache dans le cache CloudFront périphérique, lorsque la réponse a été générée par une fonction déclenchée par un événement de demande d'origine
- Connectez-vous CloudFront Journaux d'accès (journaux standard)

Si la valeur `status` n'est pas comprise entre 200 et 599, CloudFront renvoie une erreur à l'utilisateur.

`statusDescription`

Description que vous souhaitez CloudFront renvoyer dans la réponse, pour accompagner le code d'état HTTP. Vous n'avez pas besoin d'utiliser de descriptions standard, telles que `OK` pour un code de statut HTTP 200. La mise à jour de ce champ ne fonctionnera que si le client se connecte HTTP/1.1. Si le client se connecteHTTP/2, toute modification apportée au `statusDescription` sera ignorée et la description standard sera renvoyée au client.

Erreurs

Voici des erreurs possibles pour les réponses HTTP générées.

La réponse contient un corps et un code de statut HTTP 204 (Pas de contenu)

Lorsqu'une fonction est déclenchée par une demande d'affichage, CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) au visualiseur lorsque les deux conditions suivantes sont vraies :

- La valeur du code `status` est 204 (Pas de contenu)
- La réponse inclut une valeur pour `body`

Cela vient du fait que Lambda@Edge impose la restriction facultative incluse dans la RFC 2616, qui stipule qu'une réponse `HTTP 204` n'a pas besoin d'inclure de corps de message.

Restrictions concernant la taille de la réponse générée

La taille maximale d'une réponse générée par une fonction Lambda dépend de l'événement qui a déclenché la fonction :

- Événements de demande utilisateur – 40 Ko
- Événements de demande à l'origine – 1 Mo

Si la réponse est supérieure à la taille autorisée, CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) au visualiseur.

Champs obligatoires

Le champ `status` est obligatoire.

Tous les autres champs sont facultatifs.

Mise à jour des réponses HTTP dans des déclencheurs de réponse de l’origine

Lorsque CloudFront vous recevez une réponse HTTP du serveur d'origine, si un déclencheur de réponse d'origine est associé au comportement du cache, vous pouvez modifier la réponse HTTP pour remplacer ce qui a été renvoyé par l'origine.

Les scénarios courants pour mettre à jour des réponses HTTP sont les suivants :

- Modification du statut sur HTTP 200 et création d'un contenu de corps statique à renvoyer à l'utilisateur lorsqu'une origine renvoie un code de statut d'erreur (4xx ou 5xx). Pour un exemple de code, consultez Exemple : utilisation d’un déclencheur de réponse de l’origine pour mettre à jour le code de statut d’erreur sur 200.
- Modification du statut pour définir un code de statut HTTP 301 ou HTTP 302, afin de rediriger l'utilisateur vers un autre site web lorsqu'une origine renvoie un code de statut d'erreur (4xx ou

5xx). Pour un exemple de code, consultez Exemple : utilisation d'un déclencheur de réponse de l'origine pour mettre à jour le code de statut d'erreur sur 302.

> **Note**
>
> La fonction doit renvoyer une valeur d'état comprise entre `200` et `599` (inclus), sinon elle CloudFront renvoie une erreur au visualiseur.

Vous pouvez également remplacer les réponses HTTP dans les événements de requête utilisateur et à l'origine. Pour plus d'informations, consultez Génération de réponses HTTP dans les déclencheurs de demande.

Lorsque vous utilisez la réponse HTTP, Lambda@Edge n'expose pas le corps renvoyé par le serveur d'origine au déclencheur de réponse de l'origine. Vous pouvez générer un corps de contenu statique en lui attribuant la valeur souhaitée, ou supprimer le corps à l'intérieur de la fonction en définissant une valeur vide. Si vous n'actualisez pas le champ du corps dans votre fonction, le corps d'origine renvoyé par le serveur d'origine est renvoyé à l'utilisateur.

Accès au corps de requête en choisissant l'option Inclure le corps

Vous pouvez décider que Lambda@Edge expose le corps dans une demande pour des méthodes HTTP accessibles en écriture (POST, PUT, DELETE, etc.) afin que vous puissiez y accéder dans vos fonctions Lambda. Vous pouvez choisir un accès en lecture seule ou vous pouvez préciser que vous remplacerez le corps.

Pour activer cette option, choisissez Include Body (Inclure corps) lorsque vous créez un déclencheur CloudFront pour votre fonction qui correspond à un pour un événement de demande utilisateur ou de demande d'origine. Pour plus d'informations, consultez Ajout de déclencheurs pour une fonction Lambda@Edge, ou pour en savoir plus sur l'utilisation de Include Body (Inclure le corps) avec votre fonction, consultez Structure d'événement Lambda@Edge.

Les scénarios lorsque vous êtes susceptibles de vouloir utiliser cette fonction incluent les éléments suivants :

- Traitement des formulaires Web, comme « Contactez-nous », sans renvoyer les données saisies par le client aux serveurs d'origine.
- Collecte des données de balise web envoyées par les navigateurs des utilisateurs et traitement de ces données en périphérie.

Pour un exemple de code, consultez Exemples de fonctions Lambda@Edge.

> **Note**
>
> Si le corps de la demande est grand, Lambda@Edge le tronque. Pour plus d'informations sur la taille maximale et la troncature, consultez Restrictions relatives au corps de la requête avec l'option Inclure le corps.

Exemples de fonctions Lambda@Edge

Consultez les exemples suivants pour utiliser les fonctions Lambda avec Amazon. CloudFront

> **Note**
>
> Si vous choisissez Runtime Node.js 18 ou une version ultérieure pour votre fonction Lambda @Edge, un `index.mjs` fichier est créé automatiquement pour vous. Pour utiliser les exemples de code suivants, renommez plutôt le fichier `index.mjs` en `index.js`.

Rubriques

- Exemples généraux
- Génération de réponses : exemples
- Chaînes de requête - exemples
- Personnalisation de contenu à l'aide des en-têtes Pays ou Type d'appareil – exemples
- Content-based sélection dynamique de l'origine - exemples
- Mise à jour des statuts d'erreur : exemples
- Accès au corps de requête - exemples

Exemples généraux

Les exemples suivants montrent les méthodes courantes d'utilisation de Lambda @Edge dans. CloudFront

Rubriques

- Exemple : A/B test

- Exemple : remplacement d'un en-tête de réponse

Exemple : A/B test

Vous pouvez utiliser l'exemple suivant pour tester deux versions différentes d'une image sans créer de redirections ni modifier l'URL. Cet exemple lit les cookies dans la demande de l'utilisateur et modifie l'URL de la demande en conséquence. Si l'utilisateur n'envoie pas de cookie avec l'une des valeurs attendues, l'exemple affecte de façon aléatoire l'utilisateur à l'une des URL.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;

    if (request.uri !== '/experiment-pixel.jpg') {
        // do not process if this is not an A-B test request
        callback(null, request);
        return;
    }

    const cookieExperimentA = 'X-Experiment-Name=A';
    const cookieExperimentB = 'X-Experiment-Name=B';
    const pathExperimentA = '/experiment-group/control-pixel.jpg';
    const pathExperimentB = '/experiment-group/treatment-pixel.jpg';

    /*
     * Lambda at the Edge headers are array objects.
     *
     * When a client sends multiple headers with the same name, each
     * header is a separate entry in the array. For example:
     * > GET /viewerRes/test HTTP/1.1
     * > X-Custom: valueA
     * > X-Custom: valueB
     *
     * You can access the first at headers["x-custom"][0].value
     * and the second at headers["x-custom"][1].value.
     *
     * CloudFront concatenates multiple Cookie headers into a single entry,
 separated by "; ".
```

```
     * For example:
     * > Cookie: First=1; Second=2
     * > Cookie: ClientCode=abc
     *
     * becomes headers["cookie"][0].value = "First=1; Second=2; ClientCode=abc"
     * This behavior is consistent across HTTP/1.1, HTTP/2, and HTTP/3.
     *
     * Header values are not parsed.
     */
    let experimentUri;
    if (headers.cookie) {
        for (let i = 0; i < headers.cookie.length; i++) {
            if (headers.cookie[i].value.indexOf(cookieExperimentA) >= 0) {
                console.log('Experiment A cookie found');
                experimentUri = pathExperimentA;
                break;
            } else if (headers.cookie[i].value.indexOf(cookieExperimentB) >= 0) {
                console.log('Experiment B cookie found');
                experimentUri = pathExperimentB;
                break;
            }
        }
    }

    if (!experimentUri) {
        console.log('Experiment cookie has not been found. Throwing dice...');
        if (Math.random() < 0.75) {
            experimentUri = pathExperimentA;
        } else {
            experimentUri = pathExperimentB;
        }
    }

    request.uri = experimentUri;
    console.log(`Request uri set to "${request.uri}"`);
    callback(null, request);
};
```

Python

```
import json
import random
```

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    if request['uri'] != '/experiment-pixel.jpg':
        # Not an A/B Test
        return request

    cookieExperimentA, cookieExperimentB = 'X-Experiment-Name=A', 'X-Experiment-
Name=B'
    pathExperimentA, pathExperimentB = '/experiment-group/control-pixel.jpg', '/
experiment-group/treatment-pixel.jpg'

    '''
    Lambda at the Edge headers are array objects.

    When a client sends multiple headers with the same name, each
    header is a separate entry in the array. For example:
    > GET /viewerRes/test HTTP/1.1
    > X-Custom: valueA
    > X-Custom: valueB

    You can access the first at headers["x-custom"][0].value
    and the second at headers["x-custom"][1].value.

    CloudFront concatenates multiple Cookie headers into a single entry, separated
 by "; ".
    For example:
    > Cookie: First=1; Second=2
    > Cookie: ClientCode=abc

    becomes headers["cookie"][0].value = "First=1; Second=2; ClientCode=abc"
    This behavior is consistent across HTTP/1.1, HTTP/2, and HTTP/3.

    Header values are not parsed.
    '''

    experimentUri = ""

    for cookie in headers.get('cookie', []):
        if cookieExperimentA in cookie['value']:
            print("Experiment A cookie found")
            experimentUri = pathExperimentA
            break
```

```
        elif cookieExperimentB in cookie['value']:
            print("Experiment B cookie found")
            experimentUri = pathExperimentB
            break

    if not experimentUri:
        print("Experiment cookie has not been found. Throwing dice...")
        if random.random() < 0.75:
            experimentUri = pathExperimentA
        else:
            experimentUri = pathExperimentB

    request['uri'] = experimentUri
    print(f"Request uri set to {experimentUri}")
    return request
```

Exemple : remplacement d'un en-tête de réponse

L'exemple suivant montre comment changer la valeur d'un en-tête de réponse en fonction de la valeur d'un autre en-tête.

Node.js

```
export const handler = async (event) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;

    const headerNameSrc = 'X-Amz-Meta-Last-Modified';
    const headerNameDst = 'Last-Modified';

    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameDst.toLowerCase()] = [{
            key: headerNameDst,
            value: headers[headerNameSrc.toLowerCase()][0].value,
        }];
        console.log(`Response header "${headerNameDst}" was set to ` +
                    `"${headers[headerNameDst.toLowerCase()][0].value}"`);
    }

    return response;
};
```

Python

```
import json

def lambda_handler(event, context):
    response = event['Records'][0]['cf']['response']
    headers = response['headers']

    header_name_src = 'X-Amz-Meta-Last-Modified'
    header_name_dst = 'Last-Modified'

    if headers.get(header_name_src.lower()):
        headers[header_name_dst.lower()] = [{
            'key': header_name_dst,
            'value': headers[header_name_src.lower()][0]['value']
        }]
        print(f'Response header "{header_name_dst}" was set to '
              f'"{headers[header_name_dst.lower()][0]["value"]}"')

    return response
```

Génération de réponses : exemples

Les exemples suivants illustrent l'utilisation de Lambda@Edge pour générer des réponses.

Rubriques

- Exemple : traitement de contenu statique (réponse générée)
- Exemple : génération d'une redirection HTTP (réponse générée)

Exemple : traitement de contenu statique (réponse générée)

L'exemple suivant montre comment utiliser une fonction Lambda pour traiter le contenu statique d'un site web, ce qui réduit la charge sur le serveur d'origine et réduit la latence globale.

> **Note**
>
> Vous pouvez générer des réponses HTTP pour les événements de requête utilisateur ou de requête à l'origine. Pour plus d'informations, consultez the section called "Génération de réponses HTTP dans les déclencheurs de demande".

Vous pouvez également remplacer ou supprimer le corps de la réponse HTTP dans les événements de réponse de l'origine. Pour plus d'informations, consultez the section called "Mise à jour des réponses HTTP dans des déclencheurs de réponse de l'origine".

Node.js

```
'use strict';

const content = `
<\!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Simple Lambda@Edge Static Content Response</title>
  </head>
  <body>
    <p>Hello from Lambda@Edge!</p>
  </body>
</html>
`;

exports.handler = (event, context, callback) => {
    /*
     * Generate HTTP OK response using 200 status code with HTML body.
     */
    const response = {
        status: '200',
        statusDescription: 'OK',
        headers: {
            'cache-control': [{
                key: 'Cache-Control',
                value: 'max-age=100'
            }],
            'content-type': [{
                key: 'Content-Type',
                value: 'text/html'
            }]
        },
        body: content,
    };
    callback(null, response);
```

```
};
```

Python

```
import json

CONTENT = """
<\!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Simple Lambda@Edge Static Content Response</title>
</head>
<body>
    <p>Hello from Lambda@Edge!</p>
</body>
</html>
"""

def lambda_handler(event, context):
    # Generate HTTP OK response using 200 status code with HTML body.
    response = {
        'status': '200',
        'statusDescription': 'OK',
        'headers': {
            'cache-control': [
                {
                    'key': 'Cache-Control',
                    'value': 'max-age=100'
                }
            ],
            "content-type": [
                {
                    'key': 'Content-Type',
                    'value': 'text/html'
                }
            ]
        },
        'body': CONTENT
    }
    return response
```

Exemple : génération d'une redirection HTTP (réponse générée)

L'exemple suivant montre comment générer une redirection HTTP.

> **Note**
>
> Vous pouvez générer des réponses HTTP pour les événements de requête utilisateur ou de requête à l'origine. Pour plus d'informations, consultez Génération de réponses HTTP dans les déclencheurs de demande.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    /*
     * Generate HTTP redirect response with 302 status code and Location header.
     */
    const response = {
        status: '302',
        statusDescription: 'Found',
        headers: {
            location: [{
                key: 'Location',
                value: 'https://docs.aws.amazon.com/lambda/latest/dg/lambda-
edge.html',
            }],
        },
    };
    callback(null, response);
};
```

Python

```
def lambda_handler(event, context):

    # Generate HTTP redirect response with 302 status code and Location header.

    response = {
        'status': '302',
        'statusDescription': 'Found',
```

```
        'headers': {
            'location': [{
                'key': 'Location',
                'value': 'https://docs.aws.amazon.com/lambda/latest/dg/lambda-
edge.html'
            }]
        }
    }

    return response
```

Chaînes de requête - exemples

Les exemples suivants montrent comment utiliser Lambda@Edge avec des chaînes de requête.

Rubriques

- Exemple : ajout d'un en-tête basé sur un paramètre de chaîne de requête
- Exemple : normalisation des paramètres de chaîne de requête pour améliorer le taux d'accès au cache
- Exemple : redirection des utilisateurs non authentifiés vers une page de connexion

Exemple : ajout d'un en-tête basé sur un paramètre de chaîne de requête

L'exemple suivant montre comment obtenir la paire clé-valeur d'un paramètre de chaîne de requête, puis ajouter un en-tête en fonction de ces valeurs.

Node.js

```
'use strict';

const querystring = require('querystring');
exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;

    /* When a request contains a query string key-value pair but the origin server
     * expects the value in a header, you can use this Lambda function to
     * convert the key-value pair to a header. Here's what the function does:
     * 1. Parses the query string and gets the key-value pair.
     * 2. Adds a header to the request using the key-value pair that the function
 got in step 1.
```

```
     */

    /* Parse request querystring to get javascript object */
    const params = querystring.parse(request.querystring);

    /* Move auth param from querystring to headers */
    const headerName = 'Auth-Header';
    request.headers[headerName.toLowerCase()] = [{ key: headerName, value:
 params.auth }];
    delete params.auth;

    /* Update request querystring */
    request.querystring = querystring.stringify(params);

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs, urlencode

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    '''
    When a request contains a query string key-value pair but the origin server
    expects the value in a header, you can use this Lambda function to
    convert the key-value pair to a header. Here's what the function does:
        1. Parses the query string and gets the key-value pair.
        2. Adds a header to the request using the key-value pair that the function
 got in step 1.
    '''

    # Parse request querystring to get dictionary/json
    params = {k : v[0] for k, v in parse_qs(request['querystring']).items()}

    # Move auth param from querystring to headers
    headerName = 'Auth-Header'
    request['headers'][headerName.lower()] = [{'key': headerName, 'value':
 params['auth']}]
    del params['auth']

    # Update request querystring
```

```
    request['querystring'] = urlencode(params)

    return request
```

Exemple : normalisation des paramètres de chaîne de requête pour améliorer le taux d'accès au cache

L'exemple suivant montre comment améliorer le taux de réussite de votre cache en apportant les modifications suivantes aux chaînes de requête avant de CloudFront transférer les demandes à votre origine :

- Classez par ordre alphabétique les paires clé-valeur selon le nom du paramètre.
- Modifiez la casse des paires clé-valeur en minuscules.

Pour plus d'informations, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête.

Node.js

```
'use strict';

const querystring = require('querystring');

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    /* When you configure a distribution to forward query strings to the origin and
     * to cache based on an allowlist of query string parameters, we recommend
     * the following to improve the cache-hit ratio:
     * - Always list parameters in the same order.
     * - Use the same case for parameter names and values.
     *
     * This function normalizes query strings so that parameter names and values
     * are lowercase and parameter names are in alphabetical order.
     *
     * For more information, see:
     * https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/
QueryStringParameters.html
     */

    console.log('Query String: ', request.querystring);
```

```
    /* Parse request query string to get javascript object */
    const params = querystring.parse(request.querystring.toLowerCase());
    const sortedParams = {};

    /* Sort param keys */
    Object.keys(params).sort().forEach(key => {
        sortedParams[key] = params[key];
    });

    /* Update request querystring with normalized  */
    request.querystring = querystring.stringify(sortedParams);

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs, urlencode

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    '''
    When you configure a distribution to forward query strings to the origin and
    to cache based on an allowlist of query string parameters, we recommend
    the following to improve the cache-hit ratio:
    Always list parameters in the same order.
    - Use the same case for parameter names and values.

    This function normalizes query strings so that parameter names and values
    are lowercase and parameter names are in alphabetical order.

    For more information, see:
    https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/
QueryStringParameters.html
    '''
    print("Query string: ", request["querystring"])

    # Parse request query string to get js object
    params = {k : v[0] for k, v in parse_qs(request['querystring'].lower()).items()}

    # Sort param keys
    sortedParams = sorted(params.items(), key=lambda x: x[0])
```

```
    # Update request querystring with normalized
    request['querystring'] = urlencode(sortedParams)

    return request
```

Exemple : redirection des utilisateurs non authentifiés vers une page de connexion

L'exemple suivant montre comment rediriger des utilisateurs vers une page de connexion s'ils n'ont pas saisi leurs informations d'identification.

Node.js

```
'use strict';

function parseCookies(headers) {
    const parsedCookie = {};
    if (headers.cookie) {
        headers.cookie[0].value.split(';').forEach((cookie) => {
            if (cookie) {
                const parts = cookie.split('=');
                parsedCookie[parts[0].trim()] = parts[1].trim();
            }
        });
    }
    return parsedCookie;
}

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;

    /* Check for session-id in request cookie in viewer-request event,
     * if session-id is absent, redirect the user to sign in page with original
     * request sent as redirect_url in query params.
     */

    /* Check for session-id in cookie, if present then proceed with request */
    const parsedCookies = parseCookies(headers);
    if (parsedCookies && parsedCookies['session-id']) {
        callback(null, request);
        return;
    }
```

```
    /* URI encode the original request to be sent as redirect_url in query params */
    const encodedRedirectUrl = encodeURIComponent(`https://
${headers.host[0].value}${request.uri}?${request.querystring}`);
    const response = {
        status: '302',
        statusDescription: 'Found',
        headers: {
            location: [{
                key: 'Location',
                value: `https://www.example.com/signin?redirect_url=
${encodedRedirectUrl}`,
            }],
        },
    };
    callback(null, response);
};
```

Python

```
import urllib

def parseCookies(headers):
    parsedCookie = {}
    if headers.get('cookie'):
        for cookie in headers['cookie'][0]['value'].split(';'):
            if cookie:
                parts = cookie.split('=')
                parsedCookie[parts[0].strip()] = parts[1].strip()
    return parsedCookie

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    '''
    Check for session-id in request cookie in viewer-request event,
    if session-id is absent, redirect the user to sign in page with original
    request sent as redirect_url in query params.
    '''

    # Check for session-id in cookie, if present, then proceed with request
    parsedCookies = parseCookies(headers)
```

```
    if parsedCookies and parsedCookies['session-id']:
        return request

    # URI encode the original request to be sent as redirect_url in query params
    redirectUrl = "https://%s%s?%s" % (headers['host'][0]['value'], request['uri'],
request['querystring'])
    encodedRedirectUrl = urllib.parse.quote_plus(redirectUrl.encode('utf-8'))

    response = {
        'status': '302',
        'statusDescription': 'Found',
        'headers': {
            'location': [{
                'key': 'Location',
                'value': 'https://www.example.com/signin?redirect_url=%s' %
encodedRedirectUrl
            }]
        }
    }
    return response
```

Personnalisation de contenu à l'aide des en-têtes Pays ou Type d'appareil – exemples

Les exemples suivants illustrent une méthode d'utilisation de Lambda@Edge pour personnaliser le comportement en fonction de l'emplacement ou du type d'appareil utilisé par l'utilisateur.

Rubriques

- Exemple : redirection de demandes utilisateur vers une URL spécifique à un pays
- Exemple : gestion de différentes versions d'un objet en fonction de l'appareil

Exemple : redirection de demandes utilisateur vers une URL spécifique à un pays

L'exemple suivant montre comment générer une réponse de redirection HTTP avec une URL propre à un pays et renvoyer la réponse à l'utilisateur. Ceci s'avère utile lorsque vous souhaitez fournir des réponses propres à un pays. Exemples :

- Si vous avez des sous-domaines propres à un pays, comme us.example.com et tw.example.com, vous pouvez générer une réponse de redirection lorsqu'un utilisateur demande example.com.

- Si vous diffusez une vidéo, mais que vous ne disposez pas de droits pour diffuser le contenu dans un pays spécifique, vous pouvez rediriger les utilisateurs de ce pays vers une page qui explique pourquoi ils ne peuvent regarder la vidéo.

Remarques :

- Vous devez configurer votre distribution pour être mise en cache en fonction de l'en-tête `CloudFront-Viewer-Country`. Pour plus d'informations, consultez Mise en cache basée sur des en-têtes de demande sélectionnés.
- CloudFront ajoute l'`CloudFront-Viewer-Country`en-tête après l'événement de demande du spectateur. Pour utiliser cet exemple, vous devez créer un déclencheur pour l'événement de demande à l'origine.

Node.js

```
'use strict';

/* This is an origin request function */
exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;

    /*
     * Based on the value of the CloudFront-Viewer-Country header, generate an
     * HTTP status code 302 (Redirect) response, and return a country-specific
     * URL in the Location header.
     * NOTE: 1. You must configure your distribution to cache based on the
     *          CloudFront-Viewer-Country header. For more information, see
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
     *       2. CloudFront adds the CloudFront-Viewer-Country header after the
 viewer
     *          request event. To use this example, you must create a trigger for
 the
     *          origin request event.
     */

    let url = 'https://example.com/';
    if (headers['cloudfront-viewer-country']) {
        const countryCode = headers['cloudfront-viewer-country'][0].value;
```

```
        if (countryCode === 'TW') {
            url = 'https://tw.example.com/';
        } else if (countryCode === 'US') {
            url = 'https://us.example.com/';
        }
    }

    const response = {
        status: '302',
        statusDescription: 'Found',
        headers: {
            location: [{
                key: 'Location',
                value: url,
            }],
        },
    };
    callback(null, response);
};
```

Python

```
# This is an origin request function

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']

    '''
    Based on the value of the CloudFront-Viewer-Country header, generate an
    HTTP status code 302 (Redirect) response, and return a country-specific
    URL in the Location header.
    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Viewer-Country header. For more information, see
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
          2. CloudFront adds the CloudFront-Viewer-Country header after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
    '''

    url = 'https://example.com/'
    viewerCountry = headers.get('cloudfront-viewer-country')
    if viewerCountry:
```

```
        countryCode = viewerCountry[0]['value']
        if countryCode == 'TW':
            url = 'https://tw.example.com/'
        elif countryCode == 'US':
            url = 'https://us.example.com/'

    response = {
        'status': '302',
        'statusDescription': 'Found',
        'headers': {
            'location': [{
                'key': 'Location',
                'value': url
            }]
        }
    }

    return response
```

Exemple : gestion de différentes versions d'un objet en fonction de l'appareil

L'exemple suivant montre comment servir différentes versions d'un objet en fonction du type d'appareil employé par l'utilisateur, par exemple, un appareil mobile ou une tablette. Remarques :

- Vous devez configurer votre distribution pour être mise en cache en fonction des en-têtes `CloudFront-Is-*-Viewer`. Pour plus d'informations, consultez Mise en cache basée sur des en-têtes de demande sélectionnés.
- CloudFront ajoute les `CloudFront-Is-*-Viewer` en-têtes après l'événement de demande du spectateur. Pour utiliser cet exemple, vous devez créer un déclencheur pour l'événement de demande à l'origine.

Node.js

```
'use strict';

/* This is an origin request function */
exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
    const headers = request.headers;
```

```
    /*
     * Serve different versions of an object based on the device type.
     * NOTE: 1. You must configure your distribution to cache based on the
     *          CloudFront-Is-*-Viewer headers. For more information, see
     *          the following documentation:
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-device-type
     *       2. CloudFront adds the CloudFront-Is-*-Viewer headers after the viewer
     *          request event. To use this example, you must create a trigger for
 the
     *          origin request event.
     */

    const desktopPath = '/desktop';
    const mobilePath = '/mobile';
    const tabletPath = '/tablet';
    const smarttvPath = '/smarttv';

    if (headers['cloudfront-is-desktop-viewer']
        && headers['cloudfront-is-desktop-viewer'][0].value === 'true') {
        request.uri = desktopPath + request.uri;
    } else if (headers['cloudfront-is-mobile-viewer']
               && headers['cloudfront-is-mobile-viewer'][0].value === 'true') {
        request.uri = mobilePath + request.uri;
    } else if (headers['cloudfront-is-tablet-viewer']
               && headers['cloudfront-is-tablet-viewer'][0].value === 'true') {
        request.uri = tabletPath + request.uri;
    } else if (headers['cloudfront-is-smarttv-viewer']
               && headers['cloudfront-is-smarttv-viewer'][0].value === 'true') {
        request.uri = smarttvPath + request.uri;
    }
    console.log(`Request uri set to "${request.uri}"`);

    callback(null, request);
};
```

Python

```
# This is an origin request function
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    headers = request['headers']
```

```
    '''
    Serve different versions of an object based on the device type.
    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Is-*-Viewer headers. For more information, see
            the following documentation:
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
            https://docs.aws.amazon.com/console/cloudfront/cache-on-device-type
          2. CloudFront adds the CloudFront-Is-*-Viewer headers after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
    '''

    desktopPath = '/desktop';
    mobilePath = '/mobile';
    tabletPath = '/tablet';
    smarttvPath = '/smarttv';

    if 'cloudfront-is-desktop-viewer' in headers and headers['cloudfront-is-desktop-
viewer'][0]['value'] == 'true':
        request['uri'] = desktopPath + request['uri']
    elif 'cloudfront-is-mobile-viewer' in headers and headers['cloudfront-is-mobile-
viewer'][0]['value'] == 'true':
        request['uri'] = mobilePath + request['uri']
    elif 'cloudfront-is-tablet-viewer' in headers and headers['cloudfront-is-tablet-
viewer'][0]['value'] == 'true':
        request['uri'] = tabletPath + request['uri']
    elif 'cloudfront-is-smarttv-viewer' in headers and headers['cloudfront-is-
smarttv-viewer'][0]['value'] == 'true':
        request['uri'] = smarttvPath + request['uri']

    print("Request uri set to %s" % request['uri'])

    return request
```

Content-based sélection dynamique de l'origine - exemples

Les exemples suivants illustrent une méthode d’utilisation de Lambda@Edge pour acheminer vers différentes origines en fonction des informations contenues dans la demande.

Rubriques

- Exemple : utilisation d'un déclencheur de demande à l'origine pour passer d'une origine personnalisée à une origine Amazon S3
- Exemple : utilisation d'un déclencheur de demande à l'origine pour modifier la région de l'origine Amazon S3
- Exemple : utilisation d'un déclencheur de demande à l'origine pour passer d'une origine Amazon S3 à une origine personnalisée
- Exemple : utilisation d'un déclencheur de demande à l'origine pour transférer progressivement le trafic d'un compartiment Amazon S3 à un autre
- Exemple : utilisation d'un déclencheur de demande à l'origine pour modifier le nom de domaine de l'origine en fonction de l'en-tête du pays

Exemple : utilisation d'un déclencheur de demande à l'origine pour passer d'une origine personnalisée à une origine Amazon S3

Cette fonction explique comment un déclencheur de demande à l'origine peut être utilisé pour passer d'une origine personnalisée à une origine Amazon S3 à partir de laquelle le contenu est récupéré en fonction des propriétés de la demande.

Node.js

```
'use strict';

 const querystring = require('querystring');

 exports.handler = (event, context, callback) => {
     const request = event.Records[0].cf.request;

     /**
      * Reads query string to check if S3 origin should be used, and
      * if true, sets S3 origin properties.
      */

     const params = querystring.parse(request.querystring);

     if (params['useS3Origin']) {
         if (params['useS3Origin'] === 'true') {
             const s3DomainName = 'amzn-s3-demo-bucket.s3.amazonaws.com';

             /* Set S3 origin fields */
```

```
            request.origin = {
                s3: {
                    domainName: s3DomainName,
                    region: '',
                    authMethod: 'origin-access-identity',
                    path: '',
                    customHeaders: {}
                }
            };
            request.headers['host'] = [{ key: 'host', value: s3DomainName}];
        }
    }

    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    '''
    Reads query string to check if S3 origin should be used, and
    if true, sets S3 origin properties
    '''
    params = {k: v[0] for k, v in parse_qs(request['querystring']).items()}
    if params.get('useS3Origin') == 'true':
        s3DomainName = 'amzn-s3-demo-bucket.s3.amazonaws.com'

        # Set S3 origin fields
        request['origin'] = {
            's3': {
                'domainName': s3DomainName,
                'region': '',
                'authMethod': 'origin-access-identity',
                'path': '',
                'customHeaders': {}
            }
        }
        request['headers']['host'] = [{'key': 'host', 'value': s3DomainName}]
    return request
```

Exemple : utilisation d’un déclencheur de demande à l’origine pour modifier la région de l’origine Amazon S3

Cette fonction explique comment un déclencheur de demande à l'origine peut être utilisé pour modifier l'origine Amazon S3 à partir de laquelle le contenu est récupéré en fonction des propriétés de la demande.

Dans cet exemple, vous utilisez la valeur de l'`CloudFront-Viewer-Country`en-tête pour mettre à jour le nom de domaine du compartiment S3 en un compartiment situé dans une région plus proche de l'utilisateur. Cela peut être utile à plusieurs égards :

- Cela réduit la latence lorsque la région spécifiée est plus proche du pays de l'utilisateur.
- Il est possible de contrôler les données en s'assurant qu'elles sont distribuées depuis une origine qui se trouve dans le pays de provenance de la demande.

Pour utiliser cet exemple, vous devez procéder comme suit :

- Vous devez configurer votre distribution à mettre en cache en fonction de l'en-tête `CloudFront-Viewer-Country`. Pour plus d’informations, consultez Mise en cache basée sur des en-têtes de demande sélectionnés.
- Créez un déclencheur pour cette fonction dans l'événement de demande d'origine. CloudFrontajoute l'`CloudFront-Viewer-Country`en-tête après l'événement de demande du visualiseur. Pour utiliser cet exemple, vous devez vous assurer que la fonction s'exécute pour une demande d'origine.

> **Note**
>
> L’exemple de code suivant utilise la même identité d’accès d’origine (OAI) pour tous les compartiments S3 que vous utilisez comme origine. Pour plus d’informations, consultez Identité d’accès d’origine.

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;
```

```
    /**
     * This blueprint demonstrates how an origin-request trigger can be used to
     * change the origin from which the content is fetched, based on request
 properties.
     * In this example, we use the value of the CloudFront-Viewer-Country header
     * to update the S3 bucket domain name to a bucket in a Region that is closer to
     * the viewer.
     *
     * This can be useful in several ways:
     *      1) Reduces latencies when the Region specified is nearer to the viewer's
     *         country.
     *      2) Provides data sovereignty by making sure that data is served from an
     *         origin that's in the same country that the request came from.
     *
     * NOTE: 1. You must configure your distribution to cache based on the
     *          CloudFront-Viewer-Country header. For more information, see
     *          https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-
headers
     *       2. CloudFront adds the CloudFront-Viewer-Country header after the
 viewer
     *          request event. To use this example, you must create a trigger for
 the
     *          origin request event.
     */

    const countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    };

    if (request.headers['cloudfront-viewer-country']) {
        const countryCode = request.headers['cloudfront-viewer-country'][0].value;
        const region = countryToRegion[countryCode];

        /**
         * If the viewer's country is not in the list you specify, the request
         * goes to the default S3 bucket you've configured.
         */
        if (region) {
```

```
            /**
             * If you've set up OAI, the bucket policy in the destination bucket
             * should allow the OAI GetObject operation, as configured by default
             * for an S3 origin with OAI. Another requirement with OAI is to provide
             * the Region so it can be used for the SIGV4 signature. Otherwise, the
             * Region is not required.
             */
            request.origin.s3.region = region;
            const domainName = `amzn-s3-demo-bucket-in-${region}.s3.
${region}.amazonaws.com`;
            request.origin.s3.domainName = domainName;
            request.headers['host'] = [{ key: 'host', value: domainName }];
        }
    }

    callback(null, request);
};
```

Python

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    '''
    This blueprint demonstrates how an origin-request trigger can be used to
    change the origin from which the content is fetched, based on request
 properties.
    In this example, we use the value of the CloudFront-Viewer-Country header
    to update the S3 bucket domain name to a bucket in a Region that is closer to
    the viewer.

    This can be useful in several ways:
        1) Reduces latencies when the Region specified is nearer to the viewer's
            country.
        2) Provides data sovereignty by making sure that data is served from an
            origin that's in the same country that the request came from.

    NOTE: 1. You must configure your distribution to cache based on the
            CloudFront-Viewer-Country header. For more information, see
            https://docs.aws.amazon.com/console/cloudfront/cache-on-selected-headers
          2. CloudFront adds the CloudFront-Viewer-Country header after the viewer
            request event. To use this example, you must create a trigger for the
            origin request event.
```

```
    '''

    countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    }

    viewerCountry = request['headers'].get('cloudfront-viewer-country')
    if viewerCountry:
        countryCode = viewerCountry[0]['value']
        region = countryToRegion.get(countryCode)

        # If the viewer's country in not in the list you specify, the request
        # goes to the default S3 bucket you've configured
        if region:
            '''
            If you've set up OAI, the bucket policy in the destination bucket
            should allow the OAI GetObject operation, as configured by default
            for an S3 origin with OAI. Another requirement with OAI is to provide
            the Region so it can be used for the SIGV4 signature. Otherwise, the
            Region is not required.
            '''
            request['origin']['s3']['region'] = region
            domainName = 'amzn-s3-demo-bucket-in-{0}.s3.
{0}.amazonaws.com'.format(region)
            request['origin']['s3']['domainName'] = domainName
            request['headers']['host'] = [{'key': 'host', 'value': domainName}]

    return request
```

Exemple : utilisation d’un déclencheur de demande à l’origine pour passer d’une origine Amazon S3 à une origine personnalisée

Cette fonction explique comment un déclencheur de demande à l'origine peut être utilisé pour modifier l'origine personnalisée à partir de laquelle le contenu est récupéré, en fonction des propriétés de la demande.

Node.js

```
'use strict';

const querystring = require('querystring');

 exports.handler = (event, context, callback) => {
     const request = event.Records[0].cf.request;

     /**
      * Reads query string to check if custom origin should be used, and
      * if true, sets custom origin properties.
      */

     const params = querystring.parse(request.querystring);

     if (params['useCustomOrigin']) {
         if (params['useCustomOrigin'] === 'true') {

             /* Set custom origin fields*/
             request.origin = {
                 custom: {
                     domainName: 'www.example.com',
                     port: 443,
                     protocol: 'https',
                     path: '',
                     sslProtocols: ['TLSv1', 'TLSv1.1'],
                     readTimeout: 5,
                     keepaliveTimeout: 5,
                     customHeaders: {}
                 }
             };
             request.headers['host'] = [{ key: 'host', value: 'www.example.com'}];
         }
     }
    callback(null, request);
};
```

Python

```
from urllib.parse import parse_qs

def lambda_handler(event, context):
```

```
    request = event['Records'][0]['cf']['request']

    # Reads query string to check if custom origin should be used, and
    # if true, sets custom origin properties

    params = {k: v[0] for k, v in parse_qs(request['querystring']).items()}

    if params.get('useCustomOrigin') == 'true':
            # Set custom origin fields
            request['origin'] = {
                'custom': {
                    'domainName': 'www.example.com',
                    'port': 443,
                    'protocol': 'https',
                    'path': '',
                    'sslProtocols': ['TLSv1', 'TLSv1.1'],
                    'readTimeout': 5,
                    'keepaliveTimeout': 5,
                    'customHeaders': {}
                }
            }
            request['headers']['host'] = [{'key': 'host', 'value':
 'www.example.com'}]

    return request
```

Exemple : utilisation d'un déclencheur de demande à l'origine pour transférer progressivement le trafic d'un compartiment Amazon S3 à un autre

Cette fonction explique comment vous pouvez transférer progressivement le trafic d'un compartiment Amazon S3 à un autre de manière contrôlée.

Node.js

```
'use strict';

    function getRandomInt(min, max) {
        /* Random number is inclusive of min and max*/
        return Math.floor(Math.random() * (max - min + 1)) + min;
 }

exports.handler = (event, context, callback) => {
```

```
    const request = event.Records[0].cf.request;
    const BLUE_TRAFFIC_PERCENTAGE = 80;

    /**
      * This Lambda function demonstrates how to gradually transfer traffic from
      * one S3 bucket to another in a controlled way.
      * We define a variable BLUE_TRAFFIC_PERCENTAGE which can take values from
      * 1 to 100. If the generated randomNumber less than or equal to
 BLUE_TRAFFIC_PERCENTAGE, traffic
      * is re-directed to blue-bucket. If not, the default bucket that we've
 configured
      * is used.
      */

    const randomNumber = getRandomInt(1, 100);

if (randomNumber <= BLUE_TRAFFIC_PERCENTAGE) {
         const domainName = 'blue-bucket.s3.amazonaws.com';
         request.origin.s3.domainName = domainName;
         request.headers['host'] = [{ key: 'host', value: domainName}];
     }
    callback(null, request);
};
```

Python

```
import math
import random

def getRandomInt(min, max):
    # Random number is inclusive of min and max
    return math.floor(random.random() * (max - min + 1)) + min

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    BLUE_TRAFFIC_PERCENTAGE = 80

    '''
    This Lambda function demonstrates how to gradually transfer traffic from
    one S3 bucket to another in a controlled way.
    We define a variable BLUE_TRAFFIC_PERCENTAGE which can take values from
    1 to 100. If the generated randomNumber less than or equal to
 BLUE_TRAFFIC_PERCENTAGE, traffic
```

```
    is re-directed to blue-bucket. If not, the default bucket that we've configured
    is used.
    '''

    randomNumber = getRandomInt(1, 100)

    if randomNumber <= BLUE_TRAFFIC_PERCENTAGE:
        domainName = 'blue-bucket.s3.amazonaws.com'
        request['origin']['s3']['domainName'] = domainName
        request['headers']['host'] = [{'key': 'host', 'value': domainName}]

    return request
```

Exemple : utilisation d'un déclencheur de demande à l'origine pour modifier le nom de domaine de l'origine en fonction de l'en-tête du pays

Cette fonction explique comment vous pouvez modifier le nom de domaine de l'origine en fonction de l'en-tête `CloudFront-Viewer-Country` afin que le contenu soit transmis depuis une origine plus proche du pays de l'utilisateur.

La mise en œuvre de cette fonctionnalité pour votre distribution peut avoir les avantages suivants :

- Réduction de la latence lorsque la région spécifiée est plus proche du pays de l'utilisateur
- Assurance de la souveraineté des données en veillant à ce que les données soient distribuées depuis une origine qui se trouve dans le pays d'où vient la demande

Notez que pour activer cette fonctionnalité, vous devez configurer votre distribution pour qu'elle soit mise en cache en fonction de l'en-tête `CloudFront-Viewer-Country`. Pour plus d'informations, consultez the section called "Mise en cache basée sur des en-têtes de demande sélectionnés".

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
     const request = event.Records[0].cf.request;

  if (request.headers['cloudfront-viewer-country']) {
        const countryCode = request.headers['cloudfront-viewer-country'][0].value;
```

```
        if (countryCode === 'GB' || countryCode === 'DE' || countryCode === 'IE' )
 {
            const domainName = 'eu.example.com';
            request.origin.custom.domainName = domainName;
            request.headers['host'] = [{key: 'host', value: domainName}];
        }
     }

    callback(null, request);
};
```

Python

```
def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    viewerCountry = request['headers'].get('cloudfront-viewer-country')
    if viewerCountry:
        countryCode = viewerCountry[0]['value']
        if countryCode == 'GB' or countryCode == 'DE' or countryCode == 'IE':
            domainName = 'eu.example.com'
            request['origin']['custom']['domainName'] = domainName
            request['headers']['host'] = [{'key': 'host', 'value': domainName}]
    return request
```

Mise à jour des statuts d’erreur : exemples

Les exemples suivants fournissent des conseils sur l’utilisation de Lambda@Edge pour modifier le statut d’erreur qui est renvoyé aux utilisateurs.

Rubriques

- Exemple : utilisation d’un déclencheur de réponse de l’origine pour mettre à jour le code de statut d’erreur sur 200
- Exemple : utilisation d’un déclencheur de réponse de l’origine pour mettre à jour le code de statut d’erreur sur 302

Exemple : utilisation d’un déclencheur de réponse de l’origine pour mettre à jour le code de statut d’erreur sur 200

Cette fonction explique comment vous pouvez mettre à jour le statut de la réponse sur 200 et générer un contenu de corps statique à renvoyer à l'utilisateur dans le scénario suivant :

- La fonction est déclenchée dans une réponse de l'origine.
- Le statut de la réponse du serveur d’origine est un code de statut d’erreur (4xx ou 5xx).

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const response = event.Records[0].cf.response;

    /**
     * This function updates the response status to 200 and generates static
     * body content to return to the viewer in the following scenario:
     * 1. The function is triggered in an origin response
     * 2. The response status from the origin server is an error status code (4xx or
 5xx)
     */

    if (response.status >= 400 && response.status <= 599) {
        response.status = 200;
        response.statusDescription = 'OK';
        response.body = 'Body generation example';
    }

    callback(null, response);
};
```

Python

```
def lambda_handler(event, context):
    response = event['Records'][0]['cf']['response']

    '''
    This function updates the response status to 200 and generates static
    body content to return to the viewer in the following scenario:
```

```
    1. The function is triggered in an origin response
    2. The response status from the origin server is an error status code (4xx or
 5xx)
    '''

    if int(response['status']) >= 400 and int(response['status']) <= 599:
        response['status'] = 200
        response['statusDescription'] = 'OK'
        response['body'] = 'Body generation example'
    return response
```

Exemple : utilisation d'un déclencheur de réponse de l'origine pour mettre à jour le code de statut d'erreur sur 302

Cette fonction explique comment vous pouvez mettre à jour le code de statut HTTP sur 302 pour rediriger le trafic vers un autre chemin (comportement de cache) qui possède une autre origine configurée. Remarques :

- La fonction est déclenchée dans une réponse de l'origine.
- Le statut de la réponse du serveur d'origine est un code de statut d'erreur (4xx ou 5xx).

Node.js

```
'use strict';

exports.handler = (event, context, callback) => {
    const response = event.Records[0].cf.response;
    const request = event.Records[0].cf.request;

    /**
     * This function updates the HTTP status code in the response to 302, to
 redirect to another
     * path (cache behavior) that has a different origin configured. Note the
 following:
     * 1. The function is triggered in an origin response
     * 2. The response status from the origin server is an error status code (4xx or
 5xx)
     */

    if (response.status >= 400 && response.status <= 599) {
        const redirect_path = `/plan-b/path?${request.querystring}`;
```

```
        response.status = 302;
        response.statusDescription = 'Found';

        /* Drop the body, as it is not required for redirects */
        response.body = '';
        response.headers['location'] = [{ key: 'Location', value: redirect_path }];
    }

    callback(null, response);
};
```

Python

```
def lambda_handler(event, context):
    response = event['Records'][0]['cf']['response']
    request = event['Records'][0]['cf']['request']

    '''
    This function updates the HTTP status code in the response to 302, to redirect
 to another
    path (cache behavior) that has a different origin configured. Note the
 following:
    1. The function is triggered in an origin response
    2. The response status from the origin server is an error status code (4xx or
 5xx)
    '''

    if int(response['status']) >= 400 and int(response['status']) <= 599:
        redirect_path = '/plan-b/path?%s' % request['querystring']

        response['status'] = 302
        response['statusDescription'] = 'Found'

        # Drop the body as it is not required for redirects
        response['body'] = ''
        response['headers']['location'] = [{'key': 'Location', 'value':
 redirect_path}]

    return response
```

Accès au corps de requête - exemples

Les exemples suivants illustrent l'utilisation de Lambda@Edge pour utiliser des demandes POST.

> **Note**
>
> Pour utiliser ces exemples, vous devez activer l'option Inclure le corps dans l'association de fonction Lambda de la distribution. Elle n'est pas activée par défaut.
>
> - Pour activer ce paramètre dans la CloudFront console, cochez la case Inclure le corps dans l'association de fonctions Lambda.
> - Pour activer ce paramètre dans l' CloudFront API ou avec CloudFormation, définissez le `IncludeBody` champ sur `true` in`LambdaFunctionAssociation`.

Rubriques

- Exemple : utilisation d'un déclencheur de demande pour lire un formulaire HTML
- Exemple : utilisation d'un déclencheur de demande pour modifier un formulaire HTML

Exemple : utilisation d'un déclencheur de demande pour lire un formulaire HTML

Cette fonction montre comment vous pouvez traiter le corps d'une requête POST générée par un formulaire HTML (formulaire web), tel que « Contactez-nous ». Par exemple, vous pouvez avoir un formulaire HTML comme le suivant :

```
<html>
  <form action="https://example.com" method="post">
    Param 1: <input type="text" name="name1"><br>
    Param 2: <input type="text" name="name2"><br>
    input type="submit" value="Submit">
  </form>
</html>
```

Pour l'exemple de fonction qui suit, la fonction doit être déclenchée dans une requête d'utilisateur CloudFront ou une requête d'origine.

Node.js

```
'use strict';
```

```
const querystring = require('querystring');

/**
 * This function demonstrates how you can read the body of a POST request
 * generated by an HTML form (web form). The function is triggered in a
 * CloudFront viewer request or origin request event type.
 */

exports.handler = (event, context, callback) => {
    const request = event.Records[0].cf.request;

    if (request.method === 'POST') {
        /* HTTP body is always passed as base64-encoded string. Decode it. */
        const body = Buffer.from(request.body.data, 'base64').toString();

        /* HTML forms send the data in query string format. Parse it. */
        const params = querystring.parse(body);

        /* For demonstration purposes, we only log the form fields here.
         * You can put your custom logic here. For example, you can store the
         * fields in a database, such as Amazon DynamoDB, and generate a response
         * right from your Lambda@Edge function.
         */
        for (let param in params) {
            console.log(`For "${param}" user submitted "${params[param]}".\n`);
        }
    }
    return callback(null, request);
};
```

Python

```
import base64
from urllib.parse import parse_qs

'''
Say there is a POST request body generated by an HTML such as:

<html>
<form action="https://example.com" method="post">
    Param 1: <input type="text" name="name1"><br>
    Param 2: <input type="text" name="name2"><br>
```

```
    input type="submit" value="Submit">
</form>
</html>

'''

'''
This function demonstrates how you can read the body of a POST request
generated by an HTML form (web form). The function is triggered in a
CloudFront viewer request or origin request event type.
'''

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']

    if request['method'] == 'POST':
        # HTTP body is always passed as base64-encoded string. Decode it
        body = base64.b64decode(request['body']['data'])

        # HTML forms send the data in query string format. Parse it
        params = {k: v[0] for k, v in parse_qs(body).items()}

        '''
        For demonstration purposes, we only log the form fields here.
        You can put your custom logic here. For example, you can store the
        fields in a database, such as Amazon DynamoDB, and generate a response
        right from your Lambda@Edge function.
        '''
        for key, value in params.items():
            print("For %s use submitted %s" % (key, value))

    return request
```

Exemple : utilisation d'un déclencheur de demande pour modifier un formulaire HTML

Cette fonction montre comment vous pouvez modifier le corps d'une requête POST générée par un formulaire HTML (formulaire web). La fonction est déclenchée dans une demande de CloudFront visualisation ou une demande d'origine.

Node.js

```
'use strict';
```

```
const querystring = require('querystring');

exports.handler = (event, context, callback) => {
    var request = event.Records[0].cf.request;
    if (request.method === 'POST') {
        /* Request body is being replaced. To do this, update the following
        /* three fields:
         *    1) body.action to 'replace'
         *    2) body.encoding to the encoding of the new data.
         *
         *       Set to one of the following values:
         *
         *           text - denotes that the generated body is in text format.
         *               Lambda@Edge will propagate this as is.
         *           base64 - denotes that the generated body is base64 encoded.
         *               Lambda@Edge will base64 decode the data before sending
         *               it to the origin.
         *    3) body.data to the new body.
         */
        request.body.action = 'replace';
        request.body.encoding = 'text';
        request.body.data = getUpdatedBody(request);
    }
    callback(null, request);
};

function getUpdatedBody(request) {
    /* HTTP body is always passed as base64-encoded string. Decode it. */
    const body = Buffer.from(request.body.data, 'base64').toString();

    /* HTML forms send data in query string format. Parse it. */
    const params = querystring.parse(body);

    /* For demonstration purposes, we're adding one more param.
     *
     * You can put your custom logic here. For example, you can truncate long
     * bodies from malicious requests.
     */
    params['new-param-name'] = 'new-param-value';
    return querystring.stringify(params);
}
```

Python

```
import base64
from urllib.parse import parse_qs, urlencode

def lambda_handler(event, context):
    request = event['Records'][0]['cf']['request']
    if request['method'] == 'POST':
        '''
        Request body is being replaced. To do this, update the following
        three fields:
            1) body.action to 'replace'
            2) body.encoding to the encoding of the new data.

            Set to one of the following values:

                text - denotes that the generated body is in text format.
                    Lambda@Edge will propagate this as is.
                base64 - denotes that the generated body is base64 encoded.
                    Lambda@Edge will base64 decode the data before sending
                    it to the origin.
            3) body.data to the new body.
        '''
        request['body']['action'] = 'replace'
        request['body']['encoding'] = 'text'
        request['body']['data'] = getUpdatedBody(request)
    return request

def getUpdatedBody(request):
    # HTTP body is always passed as base64-encoded string. Decode it
    body = base64.b64decode(request['body']['data'])

    # HTML forms send data in query string format. Parse it
    params = {k: v[0] for k, v in parse_qs(body).items()}

    # For demonstration purposes, we're adding one more param

    # You can put your custom logic here. For example, you can truncate long
    # bodies from malicious requests
    params['new-param-name'] = 'new-param-value'
    return urlencode(params)
```

Restrictions sur les fonctions périphériques

Les rubriques suivantes décrivent les restrictions qui s'appliquent à CloudFront Functions et à Lambda @Edge. Certaines restrictions s'appliquent à toutes les fonctions Edge, tandis que d'autres s'appliquent uniquement à CloudFront Functions ou à Lambda @Edge.

Chaque rubrique fournit des informations détaillées sur les limites et les contraintes à prendre en compte lorsque vous développez et déployez des fonctions Edge avec CloudFront.

La compréhension de ces restrictions vous permet de vous assurer que vos fonctions Edge fonctionnent comme prévu et sont conformes aux fonctionnalités prises en charge.

Rubriques

- Restrictions sur toutes les fonctions périphériques
- Restrictions relatives aux CloudFront fonctions
- Restrictions sur Lambda@Edge

Pour plus d'informations sur les quotas (anciennement appelés limites), consultez Quotas relatifs aux CloudFront fonctions et Quotas sur Lambda@Edge.

Restrictions sur toutes les fonctions périphériques

Les restrictions suivantes s'appliquent à toutes les fonctions Edge, à la fois CloudFront Functions et Lambda @Edge.

Rubriques

- Compte AWS propriété
- Combiner CloudFront des fonctions avec Lambda @Edge
- Codes d'état HTTP
- En-têtes HTTP
- Chaînes de requête
- URI
- Encodage de l’URI, de la chaîne de requête et des en-têtes
- Microsoft Smooth Streaming

- Identification

Compte AWS propriété

Pour associer une fonction périphérique à une CloudFront distribution, la fonction et la distribution doivent appartenir à la même entité Compte AWS.

Combiner CloudFront des fonctions avec Lambda @Edge

Pour un comportement de cache donné, les restrictions suivantes s'appliquent :

- Chaque type d'événement (requête de l'utilisateur, requête de l'origine, réponse de l'origine et réponse de l'utilisateur) ne peut posséder qu'une association de fonctions périphériques.
- Vous ne pouvez pas combiner CloudFront Functions et Lambda @Edge dans les événements du spectateur (demande du spectateur et réponse du spectateur).

Toutes les autres combinaisons de fonctions périphériques sont autorisées. Le tableau suivant explique les combinaisons autorisées.

		CloudFront Fonctions	
		Demande utilisateur	Réponse utilisateur
Lambda@Edge	Demande utilisateur	Non autorisée	Non autorisée
	demande à l’origine	Autorisé	Autorisé
	Réponse de l'origine	Autorisé	Autorisé
	Réponse utilisateur	Non autorisée	Non autorisée

Codes d'état HTTP

CloudFront n'invoque pas de fonctions Edge pour les événements de réponse du spectateur lorsque l'origine renvoie le code d'état HTTP 400 ou supérieur.

Pour les événements de réponse d'origine, les fonctions Lambda@Edge sont appelées pour toutes les réponses d'origine, notamment lorsque l'origine renvoie un code de statut HTTP supérieur ou

supérieur à 400. Pour plus d'informations, consultez Mise à jour des réponses HTTP dans des déclencheurs de réponse de l'origine.

En-têtes HTTP

Certains en-têtes HTTP ne sont pas autorisés, ce qui signifie qu'ils ne sont pas exposés aux fonctions de périphérie et que les fonctions ne peuvent pas les ajouter. Les autres en-têtes sont en lecture seule, ce qui signifie que les fonctions peuvent les lire, sans pouvoir les ajouter, les modifier ou le supprimer.

Rubriques

- En-têtes non autorisés
- Read-only en-têtes

En-têtes non autorisés

Les en-têtes HTTP suivants ne sont pas exposés aux fonctions périphériques, et les fonctions ne peuvent pas les ajouter. Si votre fonction ajoute l'un de ces en-têtes, la CloudFront validation échoue et CloudFront renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur.

- `Connection`
- `Expect`
- `Keep-Alive`
- `Proxy-Authenticate`
- `Proxy-Authorization`
- `Proxy-Connection`
- `Trailer`
- `Upgrade`
- `X-Accel-Buffering`
- `X-Accel-Charset`
- `X-Accel-Limit-Rate`
- `X-Accel-Redirect`
- `X-Amz-Cf-*`
- `X-Amzn-Auth`

- X-Amzn-Cf-Billing
- X-Amzn-Cf-Id
- X-Amzn-Cf-Xff
- X-Amzn-Errortype
- X-Amzn-Fle-Profile
- X-Amzn-Header-Count
- X-Amzn-Header-Order
- X-Amzn-Lambda-Integration-Tag
- X-Amzn-RequestId
- X-Cache
- X-Edge-*
- X-Forwarded-Proto
- X-Real-IP
- CloudFront-Viewer-Cert-PEM
- Client-Cert
- Client-Cert-Chain

Read-only en-têtes

Les en-têtes suivants sont en lecture seule. Votre fonction peut les lire et les utiliser comme entrée de la logique de la fonction, mais elle ne peut pas modifier les valeurs. Si votre fonction ajoute ou modifie un en-tête en lecture seule, la CloudFront validation de la demande échoue et CloudFront renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur.

Read-only en-têtes dans les événements de demande des spectateurs

Les en-têtes suivants sont en lecture seule dans les événements de demande de l'utilisateur.

- CDN-Loop
- Content-Length
- Host
- Transfer-Encoding
- Via

Read-only en-têtes dans les événements de requête d'origine (Lambda @Edge uniquement)

Les en-têtes suivants sont en lecture seule dans les événements de demande d'origine, qui n'existent que dans Lambda@Edge.

- `Accept-Encoding`
- `CDN-Loop`
- `Content-Length`
- `If-Modified-Since`
- `If-None-Match`
- `If-Range`
- `If-Unmodified-Since`
- `Transfer-Encoding`
- `Via`

Read-only en-têtes dans les événements de réponse d'origine (Lambda @Edge uniquement)

Les en-têtes suivants sont en lecture seule dans les événements de réponse d'origine, qui n'existent que dans Lambda@Edge.

- `Transfer-Encoding`
- `Via`

Read-only en-têtes dans les événements de réponse des spectateurs

Les en-têtes suivants sont en lecture seule dans les événements de réponse des spectateurs pour CloudFront Functions et Lambda @Edge.

- `Warning`
- `Via`

Les en-têtes suivants sont en lecture seule dans les événements de réponse d'utilisateur pour Lambda@Edge.

- `Content-Length`
- `Content-Encoding`

- `Transfer-Encoding`

Chaînes de requête

Les restrictions suivantes s'appliquent aux fonctions qui lisent, mettent à jour ou créent une chaîne de requête dans un URI de demande.

- (Lambda@Edge uniquement) Pour accéder à la chaîne de requête dans une fonction de demande de l'origine ou de réponse de l'origine, votre stratégie de cache ou stratégie de demande de l'origine doit être définie sur Toutes pour Chaînes de requête.
- Une fonction peut créer ou mettre à jour une chaîne de requête pour les événements de demande de l'utilisateur et de demande de l'origine (les événements de demande de l'origine n'existent que dans Lambda@Edge).
- Une fonction peut lire une chaîne de requête, mais ne peut pas en créer ou en mettre à jour, pour les événements de réponse de l'origine et de réponse de l'utilisateur (les événements de réponse de l'origine n'existent que dans Lambda@Edge).
- Si une fonction crée ou met à jour une chaîne de requête, les restrictions suivantes s'appliquent :
  - La chaîne de requête mise à jour ne peut pas inclure des espaces, des caractères de contrôle ou l'identificateur de fragment (#).
  - La taille totale de l’URI, comprenant la chaîne de requête, doit être inférieure à 8 192 caractères.
  - Nous vous recommandons d'utiliser l'encodage de pourcentage pour l'URI et la chaîne de requête. Pour plus d’informations, consultez Encodage de l’URI, de la chaîne de requête et des en-têtes.

URI

Si une fonction modifie l'URI pour une demande, cela ne modifie pas le comportement du cache pour la demande ou l'origine vers laquelle la demande est transférée.

La taille totale de l’URI, comprenant la chaîne de requête, doit être inférieure à 8 192 caractères.

Encodage de l’URI, de la chaîne de requête et des en-têtes

Les valeurs de l'URI, de la chaîne de requête et des en-têtes qui sont transmises aux fonctions Edge sont UTF-8 codées. Votre fonction doit utiliser le UTF-8 codage pour l'URI, la chaîne de requête et les valeurs d'en-tête qu'elle renvoie. Le codage en pourcentage est compatible avec le UTF-8 codage.

La liste suivante explique comment CloudFront gère le codage de l'URI, de la chaîne de requête et des en-têtes :

- Lorsque les valeurs de la demande sont UTF-8 codées, les CloudFront transmet à votre fonction sans les modifier.
- Lorsque les valeurs de la demande sont ISO-8859-1 codées, CloudFront convertit les valeurs en UTF-8 codage avant de les transmettre à votre fonction.
- Lorsque les valeurs de la demande sont codées à l'aide d'un autre codage de caractères, CloudFront suppose qu'elles sont ISO-8859-1 codées et essaie de les convertir de ISO-8859-1 vers UTF-8.

> **Important**
>
> Les caractères convertis peuvent résulter d'une interprétation inexacte des valeurs de la demande de l'origine. Cela peut conduire votre fonction ou votre origine à produire un résultat indésirable.

Les valeurs de l'URI, de la chaîne de requête et des en-têtes qui sont CloudFront transmis à votre origine dépendent de la modification ou non des valeurs par une fonction :

- Si une fonction ne modifie pas l'URI, la chaîne de requête ou l'en-tête, elle CloudFront transmet les valeurs qu'elle a reçues dans la demande à votre origine.
- Si une fonction modifie l'URI, la chaîne de requête ou l'en-tête, CloudFront transmet les valeurs UTF-8 codées.

Microsoft Smooth Streaming

Vous ne pouvez pas utiliser les fonctions Edge avec une CloudFront distribution que vous utilisez pour diffuser des fichiers multimédia que vous avez transcodés au format Microsoft Smooth Streaming.

Identification

Vous ne pouvez pas ajouter de balises aux fonctions de périphérie. Pour plus d'informations sur le balisage CloudFront, consultezMarquer une CloudFront ressource.

Restrictions relatives aux CloudFront fonctions

Les restrictions suivantes s'appliquent uniquement aux CloudFront fonctions.

Table des matières

- Journaux
- Corps de la requête
- Utilisation d'informations d'identification temporaires avec l' CloudFront KeyValueStore API
- Environnement d’exécution
- Utilisation du calcul

Pour en savoir plus sur les quotas (anciennement appelés limites), consultez Quotas relatifs aux CloudFront fonctions.

Journaux

Les journaux de CloudFront fonctions dans Functions sont tronqués à 10 Ko.

Corps de la requête

CloudFront Les fonctions ne peuvent pas accéder au corps de la requête HTTP.

Utilisation d'informations d'identification temporaires avec l' CloudFront KeyValueStore API

Vous pouvez utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires (également appelées jetons de session). Les jetons de session vous permettent d'assumer temporairement un rôle Gestion des identités et des accès AWS (IAM) afin de pouvoir y accéder Services AWS.

Pour appeler l'CloudFront KeyValueStore API, utilisez un point de terminaison régional AWS STS pour renvoyer un jeton de session de version 2. Si vous utilisez le point de terminaison global pour AWS STS (`sts.amazonaws.com`), AWS STS cela générera un jeton de session version 1, qui n'est pas pris en charge par Signature Version 4A (SigV4a). Par conséquent, vous recevrez une erreur d’authentification.

Pour appeler l' CloudFront KeyValueStore API, vous pouvez utiliser les options suivantes :

AWS CLI et AWS kits de développement logiciel

Vous pouvez configurer le AWS CLI ou un AWS SDK pour utiliser des points de AWS STS terminaison régionaux. Pour plus d'informations, consultez Points de terminaison AWS STS régionalisés dans le Guide de référence des kits SDK et outils AWS .

Pour plus d'informations sur les AWS STS points de terminaison disponibles, consultez la section Régions et points de terminaison dans le Guide de l'utilisateur IAM.

SAML

Vous pouvez configurer SAML pour utiliser des points de AWS STS terminaison régionaux. Pour plus d'informations, consultez l'article de blog Comment utiliser des points de terminaison SAML régionaux pour le basculement.

API **`SetSecurityTokenServicePreferences`**

Au lieu d'utiliser un point de AWS STS terminaison régional, vous pouvez configurer le point de terminaison global AWS STS pour renvoyer les jetons de session de la version 2. Pour ce faire, utilisez l'opération SetSecurityTokenServicePreferences API pour configurer votre Compte AWS.

Example Exemple : commande de la CLI IAM

```
aws iam set-security-token-service-preferences --global-endpoint-token-version
 v2Token
```

> **Tip**
>
> Nous vous recommandons d'utiliser les points de terminaison AWS STS régionaux au lieu de cette option. Les points de terminaison régionaux offrent une meilleure disponibilité et des scénarios de basculement.

Fournisseur d'identité personnalisé

Si vous utilisez un fournisseur d'identité personnalisé qui assure la fédération et assume le rôle, utilisez l'une des options précédentes pour le système de fournisseur d'identité parent chargé de générer le jeton de session.

Environnement d’exécution

L'environnement d'exécution CloudFront Functions ne prend pas en charge l'évaluation dynamique du code et limite l'accès au réseau, au système de fichiers, aux variables d'environnement et aux minuteries. Pour plus d’informations, consultez Fonctions limitées.

> **Note**
>
> Pour être utilisée CloudFront KeyValueStore, votre CloudFront fonction doit utiliser le JavaScript runtime 2.0.

Utilisation du calcul

CloudFront Le temps d'exécution des fonctions est limité, mesuré en termes d'utilisation du calcul. L'utilisation du calcul est un nombre compris entre 0 et 100 qui indique la durée d'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une utilisation du calcul de 35 signifie que la durée d'exécution de la fonction représente 35 % du temps maximum autorisé.

Lorsque vous testez une fonction, la valeur d'utilisation du calcul figure dans la sortie de l'événement test. Pour les fonctions de production, vous pouvez consulter la métrique d'utilisation du calcul sur la page Surveillance de la CloudFront console ou dans CloudWatch.

Restrictions sur Lambda@Edge

Les restrictions suivantes s'appliquent uniquement à Lambda@Edge.

Table des matières

- Résolution DNS
- Codes d’état HTTP
- Version de la fonction Lambda
- Région Lambda
- Autorisations de rôle Lambda
- Fonctionnalités de Lambda
- Environnements d'exécution pris en charge
- CloudFront en-têtes
- Restrictions relatives au corps de la requête avec l'option Inclure le corps

- Délai de réponse et délai d'attente des connexions actives (origines personnalisées uniquement)

Pour obtenir des informations sur les quotas , consultez Quotas sur Lambda@Edge.

Résolution DNS

CloudFront effectue une résolution DNS sur le nom de domaine d'origine avant d'exécuter la fonction Lambda @Edge de votre demande d'origine. Si le service DNS de votre domaine rencontre des problèmes et ne CloudFront parvient pas à résoudre le nom de domaine pour obtenir l'adresse IP, votre fonction Lambda @Edge ne sera pas invoquée. CloudFrontrenverra un code d'état HTTP 502 (Bad Gateway) au client. Pour plus d'informations, consultez Erreur DNS (`NonS3OriginDnsError`).

Si la logique de votre fonction modifie le nom de domaine d'origine, elle CloudFront effectuera une autre résolution DNS sur le nom de domaine mis à jour une fois l'exécution de la fonction terminée.

Pour plus d'informations sur la gestion du basculement DNS, consultez Configuration du basculement DNS dans le Guide du développeur Amazon Route 53.

Codes d'état HTTP

Les fonctions Lambda @Edge pour les événements de réponse des spectateurs ne peuvent pas modifier le code d'état HTTP de la réponse, que celle-ci provienne de l'origine ou du CloudFront cache.

Version de la fonction Lambda

Vous devez utiliser une version numérotée de la fonction Lambda, et non `$LATEST` ou des alias.

Région Lambda

La fonction Lambda doit résider dans la région USA Est (Virginie du Nord).

Autorisations de rôle Lambda

Le rôle d'exécution IAM associé à la fonction Lambda doit autoriser les principaux de service `lambda.amazonaws.com` et `edgelambda.amazonaws.com` à endosser le rôle. Pour plus d'informations, consultez Définition des autorisations et rôles IAM pour Lambda@Edge.

Fonctionnalités de Lambda

Les fonctionnalités Lambda suivantes ne sont pas prises en charge par Lambda@Edge :

- Configurations de gestion de l'environnement d'exécution Lambda autres que Auto (par défaut)
- Configuration de votre fonction Lambda pour accéder à des ressources au sein de votre VPC
- Queues de lettres mortes de la fonction Lambda
- Variables d'environnement Lambda (à l'exception des variables d'environnement réservées, qui sont automatiquement prises en charge)
- Fonctions Lambda avec la Gestion des dépendances AWS Lambda à l'aide de couches
- Utilisation de AWS X-Ray
- Simultanéité allouée Lambda

> **Note**
>
> Les fonctions Lambda@Edge partagent les mêmes capacités de simultanéité régionale que toutes les fonctions Lambda. Pour plus d'informations, consultez Quotas sur Lambda@Edge.

- Création d'une fonction Lambda à l'aide d'une image de conteneur
- Fonctions Lambda utilisant l'architecture arm64
- Fonctions Lambda avec plus de 512 Mo de stockage éphémère
- Utilisation d'une clé gérée par le client pour votre package de déploiement .zip
- Self-managed Stockage de code Amazon S3

Environnements d'exécution pris en charge

Lambda @Edge prend en charge les dernières versions Node.js et les environnements d'exécution Python. Pour obtenir la liste des versions prises en charge et leurs futures dates d'obsolescence, consultez Environnements d'exécution pris en charge dans le Guide du développeur AWS Lambda .

> **Tip**
>
> - À titre de bonne pratique, privilégiez les versions les plus récentes des environnements d'exécution fournis afin de bénéficier des améliorations de performance et des nouvelles fonctionnalités.
> - Vous ne pouvez pas créer ou mettre à jour des fonctions avec des versions obsolètes de. Node.js Vous ne pouvez associer des fonctions existantes à ces versions qu'à des CloudFront distributions. Les fonctions avec ces versions qui sont associées aux

distributions continueront de s'exécuter. Nous vous recommandons toutefois de déplacer votre fonction vers des versions plus récentes de Node.js. Pour plus d'informations, consultez la politique de dépréciation de Runtime dans le Guide du AWS Lambda développeur et le calendrier de Node.js publication sur. GitHub

CloudFront en-têtes

Les fonctions Lambda @Edge peuvent lire, modifier, supprimer ou ajouter n'importe quel CloudFront en-tête répertorié dans. Ajouter des en-têtes de CloudFront demande

Remarques

- Si vous CloudFront souhaitez ajouter ces en-têtes, vous devez les configurer CloudFront pour les ajouter à l'aide d'une politique de cache ou d'une politique de demande d'origine.
- CloudFront ajoute les en-têtes après l'événement de demande du spectateur, ce qui signifie que les en-têtes ne sont pas disponibles pour les fonctions Lambda @Edge dans une requête du spectateur. Les en-têtes ne sont disponibles que pour les fonctions Lambda@Edge dans une demande d'origine et une réponse d'origine.
- Si la demande de visualisation inclut des en-têtes portant ces noms et que vous avez configuré CloudFront pour ajouter ces en-têtes à l'aide d'une politique de cache ou d'une politique de demande d'origine, les valeurs d'en-tête qui figuraient dans la demande de visualisation sont CloudFront remplacées. Viewer-facing les fonctions voient la valeur d'en-tête de la demande du visualiseur, tandis que les fonctions orientées vers l'origine voient la valeur d'en-tête ajoutée. CloudFront
- Si une fonction de demande de visualisation ajoute l'`CloudFront-Viewer-Country`en-tête, la validation échoue et CloudFront renvoie le code d'état HTTP 502 (Bad Gateway) au visualiseur.

Restrictions relatives au corps de la requête avec l'option Inclure le corps

Lorsque vous choisissez l'option Inclure le corps pour exposer le corps de la demande à votre fonction Lambda@Edge, les informations et les limites de taille suivantes s'appliquent aux parties du corps qui sont exposées ou remplacées.

- CloudFront toujours en base64 code le corps de la requête avant de l'exposer à Lambda @Edge.

- Si le corps de la requête est volumineux, CloudFront tronquez-le avant de l'exposer à Lambda @Edge, comme suit :
  - Pour les événements de requête d'utilisateur, le corps est tronqué à 40 Ko.
  - Pour les événements de requête de l'origine, le corps est tronqué à 1 Mo.
- Si vous accédez au corps de la demande en lecture seule, CloudFront envoie le corps complet de la demande d'origine à l'origine.
- Si votre fonction Lambda@Edge remplace le corps de la demande, les limites de taille suivantes s'appliquent au corps que la fonction renvoie :
  - Si la fonction Lambda@Edge renvoie le corps en texte brut :
    - Pour les événements de demande utilisateur, la limite de taille du corps est fixée à 40 Ko.
    - Pour les événements de demande à l'origine, la limite de taille du corps est fixée à 1 Mo.
  - Si la fonction Lambda@Edge renvoie le corps en tant que texte codé base64 :
    - Pour les événements de demande utilisateur, la limite de taille du corps est fixée à 53,2 Ko.
    - Pour les événements de demande à l'origine, la limite de taille du corps est fixée à 1,33 Mo.

> **Note**
>
> Si votre fonction Lambda@Edge renvoie un corps qui dépasse ces limites, votre demande échouera avec un code de statut HTTP 502 (Erreur de validation Lambda). Nous vous recommandons de mettre à jour votre fonction Lambda@Edge afin que le corps ne dépasse pas ces limites.

Délai de réponse et délai d'attente des connexions actives (origines personnalisées uniquement)

Si vous utilisez des fonctions Lambda@Edge pour définir le délai de réponse ou le délai d'attente des connexions actives pour les origines de votre distribution, assurez-vous de définir une valeur que votre origine est capable de prendre en charge. Pour plus d'informations, consultez Quotas de délai de réponse et d'attente des connexions actives.

Rapports, métriques et journaux

CloudFront propose plusieurs options pour la création de rapports, la surveillance et la journalisation de vos CloudFront ressources. Vous pouvez réaliser les tâches suivantes :

- Consultez et téléchargez des rapports pour connaître l'utilisation et l'activité de vos CloudFront distributions, notamment les rapports de facturation, les statistiques du cache, le contenu populaire et les principaux référents.
- Surveillez et suivez CloudFront, y compris vos fonctions informatiques de pointe, directement dans la CloudFront console ou à l'aide d'Amazon CloudWatch. CloudFront envoie des métriques CloudWatch pour les distributions et les fonctions de périphérie, à la fois Lambda @Edge et CloudFront Functions.
- Consultez les journaux des demandes des utilisateurs que vos CloudFront distributions reçoivent à l'aide de journaux standard ou de journaux d'accès en temps réel. Outre les journaux des demandes des utilisateurs, vous pouvez utiliser CloudWatch Logs pour obtenir les journaux de vos fonctions périphériques, à la fois Lambda @Edge et CloudFront Functions. Vous pouvez également l'utiliser AWS CloudTrail pour obtenir des journaux de l'activité de l' CloudFront API dans votre Compte AWS.
- Suivez les modifications de configuration de vos CloudFront ressources à l'aide de AWS Config.

Pour plus d’informations sur ces fonctions, consultez les rubriques suivantes.

Rubriques

- AWS rapports de facturation et d'utilisation pour CloudFront
- Afficher CloudFront les rapports dans la console
- Surveillez CloudFront les métriques avec Amazon CloudWatch
- CloudFront et journalisation des fonctions Edge
- Suivez les modifications de configuration avec AWS Config

AWS rapports de facturation et d'utilisation pour CloudFront

AWS fournit deux rapports d'utilisation pour CloudFront :

- Le rapport AWS de facturation est une vue de haut niveau de toutes les activités Services AWS que vous utilisez, y compris CloudFront.

- Le rapport AWS d'utilisation est un résumé de l'activité d'un service spécifique, agrégé par heure, jour ou mois. Il comprend également des tableaux d'utilisation qui fournissent une représentation graphique de votre CloudFront utilisation.

> **Note**
>
> Comme les autres Services AWS, vous CloudFront facture uniquement ce que vous utilisez. Pour en savoir plus, consultez PricingCloudFront (Tarification).

Rubriques

- Consultez le AWS rapport de facturation pour CloudFront
- Consultez le AWS rapport d'utilisation pour CloudFront
- Interprétez votre AWS rapports de facturation et d'utilisation pour CloudFront

Consultez le AWS rapport de facturation pour CloudFront

Vous pouvez consulter un résumé de votre AWS utilisation et de vos frais, classés par service, sur la page Factures de la AWS Billing and Cost Management console.

Pour consulter le AWS rapport de facturation

1. Connectez-vous à Console de gestion AWS et ouvrez la AWS Billing and Cost Management console à l'adresse https://console.aws.amazon.com/costmanagement/.
2. Dans le volet de navigation, choisissez Factures.
3. Choisissez une Période de facturation (par exemple, août 2023).
4. Dans l'onglet Frais par service, choisissez CloudFront, puis développez Global ou le Région AWS nom.
5. Pour télécharger un rapport de facturation détaillé au format CSV, choisissez Télécharger tout au format CSV.

Pour plus d'informations sur votre AWS facture, consultez la section Consulter votre facture dans le Guide de AWS Billing l'utilisateur.

Le rapport de facturation inclut les valeurs suivantes qui s'appliquent à CloudFront :

- ProductCode – `AmazonCloudFront`
- UsageType— L'une des valeurs suivantes :
  - Code qui identifie le type de transfert de données
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- ItemDescription— Une description du taux de facturation pour le UsageType.
- UsageStart Date et UsageEndDate : jour auquel l'utilisation s'applique, en temps universel coordonné (UTC).
- UsageQuantity— L'une des valeurs suivantes :
  - Nombre de requêtes au cours de la période spécifiée
  - Quantité de données transférée en gigaoctets
  - Nombre d'objets invalidés
  - Somme des mois au prorata pendant lesquels des certificats SSL étaient associés à des CloudFront distributions activées. Si vous avez, par exemple, un certificat associé à une distribution activée pendant un mois tout entier et un autre certificat associé à une distribution activée pendant la moitié du mois, cette valeur sera 1,5.

Consultez le AWS rapport d'utilisation pour CloudFront

AWS fournit un rapport CloudFront d'utilisation plus détaillé que le rapport de facturation mais moins détaillé que les journaux CloudFront d'accès. Le rapport d'utilisation offre des totaux de données d'utilisation par heure, jour ou mois et répertorie les opérations par région et type d'utilisation, par exemple les données transférées hors de la région Australie.

Pour consulter le AWS rapport d'utilisation

1. Connectez-vous à Console de gestion AWS et ouvrez la AWS Billing and Cost Management console à l'adresse https://console.aws.amazon.com/costmanagement/.
2. Dans le panneau de navigation, choisissez Cost Explorer.

3. Sur la page Nouveau rapport d'utilisation et de coûts, dans le volet Paramètres du rapport, choisissez une période et une granularité pour le rapport.
4. Sous Filtres, Service, sélectionnez CloudFront.
5. Sélectionnez le type d'utilisation.
6. Sous Répartition des coûts et de l'utilisation, choisissez Télécharger au format CSV.

Pour plus d'informations sur le rapport AWS d'utilisation, voir Rapport AWS d'utilisation dans le Guide de Exportations de données AWS l'utilisateur.

Le rapport CloudFront d'utilisation inclut les valeurs suivantes :

- Service – `AmazonCloudFront`
- Operation : méthode HTTP. Les valeurs incluent `DELETE`, `GET`, `HEAD`, `OPTIONS`, `PATCH`, `POST` et `PUT`.
- UsageType— L'une des valeurs suivantes :
  - Code qui identifie le type de transfert de données
  - `Invalidations`
  - `Executions-CloudFrontFunctions`
  - `KeyValueStore-APIOperations`
  - `KeyValueStore-EdgeReads`
  - `RealTimeLog-KinesisDataStream`
  - `SSL-Cert-Custom`
- Ressource : soit l'ID de la CloudFront distribution associée à l'utilisation, soit l'ID de certificat d'un certificat SSL que vous avez associé à une CloudFront distribution.
- StartTime/EndTime— Le jour auquel s'applique l'utilisation, en temps universel coordonné (UTC).
- UsageValue— 1) Le nombre de demandes pendant la période spécifiée ou 2) la quantité de données transférées en octets.

Si vous utilisez Amazon S3 comme source de CloudFront, pensez également à exécuter le rapport d'utilisation pour Amazon S3. Toutefois, si vous utilisez Amazon S3 à des fins autres que celles d'origine de vos CloudFront distributions, il est possible que la partie qui s'applique à votre CloudFront utilisation ne soit pas claire.

> **Tip**
>
> Pour obtenir des informations détaillées sur chaque demande CloudFront reçue pour vos objets, activez les journaux CloudFront d'accès pour votre distribution. Pour plus d'informations, consultez the section called “Journaux d'accès (journaux standard)”.

Pour plus d'informations sur la compréhension des CloudFront frais et des types d'utilisation figurant dans vos rapports, consultezthe section called “Interprétez votre AWS rapports de facturation et d'utilisation pour CloudFront”.

Interprétez votre AWS rapports de facturation et d'utilisation pour CloudFront

Une fois que vous avez le rapport de facturation et le rapport d'utilisation, vous pouvez utiliser cette rubrique pour comprendre comment interpréter chaque CloudFront frais qui apparaît sur votre facture et le type d'utilisation correspondant à chaque charge. Cette rubrique inclut les codes et les Région AWS abréviations qui peuvent figurer sur les deux rapports.

La plupart des codes des deux colonnes comportent une abréviation à deux lettres qui indique l’emplacement de l’activité. Dans le tableau suivant, *`region`* un code est remplacé dans votre AWS facture et dans le rapport d'utilisation par l'une des abréviations à deux lettres suivantes :

- AP : Hong Kong, Philippines, Corée du Sud, Taïwan, et Singapour (Asie-Pacifique)
- AU : Australie
- CA : Canada
- UE : Europe et Israël
- IN : Inde
- JP : Japon
- ME : Moyen-Orient
- SA : Amérique du Sud
- US : États-Unis
- ZA : Afrique du Sud

Pour plus d'informations sur la tarification par Région AWS, consultez la page CloudFront Tarification Amazon.

Remarques

- Ce tableau n'inclut pas les frais de transfert de vos objets d'un compartiment Amazon S3 vers des emplacements CloudFront périphériques. Le cas échéant, ces frais apparaissent dans la section Transfert de données AWS de votre facture AWS .
- La première colonne répertorie les frais qui apparaissent dans votre rapport de AWS facturation et explique ce que chacun signifie.
- La deuxième colonne répertorie les éléments qui apparaissent dans le rapport AWS d'utilisation et montre la corrélation entre les frais facturés et les éléments du rapport d'utilisation.

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
region-DataTransfer-Out-Bytes Nombre total d'octets servis depuis des emplacements CloudFront périphériques *region* en réponse à l'utilisateur GET et à HEAD ses demandes.	*region*-Out-Bytes-HTTP-Static: Octets servis à l'aide du protocole HTTP pour les objets dont le TTL est supérieur ou égal à 3 600 secondes. *region*-Out-Bytes-HTTPS-Static: Octets servis à l'aide du protocole HTTPS pour les objets dont le TTL est supérieur ou égal à 3 600 secondes. *region*-Out-Bytes-HTTP-Dynamic: Octets servis à l'aide du protocole HTTP pour les objets dont le TTL est inférieur à 3 600 secondes. *region*-Out-Bytes-HTTPS-Dynamic: Octets servis à l'aide du protocole HTTPS pour les objets dont le TTL est inférieur à 3 600 secondes.

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
	region-Out-Bytes-HTTP-Proxy: Octets renvoyés par les spectateurs CloudFront à l'aide du protocole HTTP en réponse aux `PUT` requêtes `DELETE` `OPTIONS` `PATCHPOST`,, et. *region*-Out-Bytes-HTTPS-Proxy: Octets renvoyés par les spectateurs CloudFron t à l'aide du protocole HTTPS en réponse aux `PUT` requêtes `DELETE` `OPTIONS` `PATCHPOST`,, et. Cela inclut les octets renvoyés par les spectateurs CloudFront à l'aide de gRPC.

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
region-DataTransfer-Out-OBytes Nombre total d'octets transférés depuis des emplacements CloudFront périphériques vers votre fonction d'origine ou de périphérie en réponse à des PUT demandes DELETE OPTIONS PATCHPOST,, et. Les frais incluent le transfert de WebSocket données du client au serveur.	*region*-Out-OBytes-HTTP-Proxy Nombre total d'octets transférés via HTTP depuis des emplacements CloudFront périphériques vers votre fonction d'origine ou de périphérie en réponse à des PUT requêtes DELETE OPTIONS PATCHPOST,, et. *region*-Out-OBytes-HTTPS-Proxy Nombre total d'octets transférés à l'aide du protocole HTTPS depuis des emplacements CloudFront périphériques vers votre fonction d'origine ou périphérique en réponse à des PUT requêtes DELETE OPTIONS PATCHPOST,, et. Cela inclut les octets transférés à l'aide de gRPC depuis des emplacements CloudFront périphériques vers votre origine ou vos CloudFront fonctions.
region-Requests-Tier1 Nombre de requêtes HTTP GET et HEAD	*region*-Requests-HTTP-Static Nombre de requêtes HTTP GET et HEAD diffusées pour des objets avec une durée de vie ≥ 3600 secondes *region*-Requests-HTTP-Dynamic Nombre de requêtes HTTP GET et HEAD diffusées pour des objets avec une durée de vie < 3600 secondes

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
region-Requests-Tier2-HTTPS Nombre de requêtes HTTPS `GET` et `HEAD`	*region*-Requests-HTTPS-Static Nombre de requêtes HTTPS `GET` et `HEAD` diffusées pour des objets avec une durée de vie ≥ 3600 secondes *region*-Requests-HTTPS-Dynamic Nombre de requêtes HTTPS `GET` et `HEAD` diffusées pour des objets avec une durée de vie < 3600 secondes
region-Requests-HTTP-Proxy Nombre de `PUT` requêtes `HTTPDELETE`,`OPTIONS`, `PATCHPOST`, et qui sont CloudFront redirigées vers votre fonction d'origine ou périphérique. Inclut également le nombre de WebSocket requêtes HTTP (`GET`requêtes avec `Upgrade: websocket` en-tête) qui sont transmises CloudFront à votre fonction d'origine ou de périphérie.	*region*-Requests-HTTP-Proxy Identique à l'article correspondant sur votre CloudFront facture.

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
region-Requests-HTTPS-Proxy Nombre de PUT requêtes HTTPSDELETE,OPTIONS, PATCHPOST, et qui sont CloudFront redirigées vers votre fonction d'origine ou périphérique. Inclut également les types de demande suivants : • Le nombre de WebSocket requêtes HTTPS (GETrequêtes avec Upgrade: websocket en-tête) qui sont transmises CloudFront à votre fonction d'origine ou de périphérie. • Nombre de demandes HTTPS gRPC.	*region*-Requests-HTTPS-Proxy Identique à l'article correspondant sur votre CloudFront facture.
region-Requests-HTTPS-Proxy-FLE Nombre de POST requêtes HTTPSDELETE, OPTIONSPATCH, et traitées avec un cryptage au niveau des champs qui est transféré CloudFront vers votre fonction d'origine ou périphérique.	*region*-Requests-HTTPS-Proxy-FLE Identique à l'article correspondant sur votre CloudFront facture.
region-Bytes-OriginShield Nombre total d'octets transférés de l'origine vers n'importe quel cache périphérique régional, y compris le cache périphérique régional activé en tant que Origin Shield.	*region*-Bytes-OriginShield Identique à l'article correspondant sur votre CloudFront facture.

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
region-OBytes-OriginShield Nombre total d’octets transférés vers l’origine depuis n’importe quel cache périphérique régional, y compris le cache périphérique régional activé en tant que Origin Shield.	*region*-OBytes-OriginShield Identique à l'article correspondant sur votre CloudFront facture.
region-Requests-OriginShield Nombre de requêtes envoyées à Origin Shield sous forme de couche progressive. Pour les demandes dynamiques (ne pouvant pas être mises en cache) qui sont transmises par proxy à l’origine, Origin Shield est toujours une couche incrémentielle. Pour les requêtes pouvant être mises en cache, Origin Shield est parfois une couche progressive. Pour plus d’informations, consultez the section called “Estimation des frais liés à Origin Shield”.	*region*-Requests-OriginShield Identique à l'article correspondant sur votre CloudFront facture.
Invalidations Les frais d'invalidation d'objets (suppression des objets des emplacements CloudFront périphériques). Pour plus d’informations, consultez Paiement d’une invalidation de fichier.	Invalidations Identique à l'article correspondant sur votre CloudFront facture.

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
SSL-Cert-Custom Les frais liés à l'utilisation d'un certificat SSL avec CloudFront un autre nom de domaine tel que example.com au lieu d'utiliser le certificat CloudFront SSL par défaut et le nom de domaine CloudFront attribué à votre distribution.	SSL-Cert-Custom Identique à l'article correspondant sur votre CloudFront facture.
RealTimeLog-KinesisDataStream Le coût correspondant au nombre de lignes générées pour les journaux d'accès en temps réel.	RealTimeLog-KinesisDataStream Identique à l'article correspondant sur votre CloudFront facture.
Executions-CloudFrontFunctions Le montant correspondant au nombre d'invocations de CloudFront fonctions.	Executions-CloudFrontFunctions Identique à l'article correspondant sur votre CloudFront facture.
region-Lambda-Edge-Request Frais correspondant au nombre d'invocations des fonctions Lambda@Edge.	***region***-Lambda-Edge-Request Identique à l'article correspondant sur votre CloudFront facture.
region-Lambda-Edge-GB-Second Frais correspondant à la durée comprise entre l'invocation de votre fonction Lambda@Edge et le moment où elle renvoie un résultat ou se termine.	***region***-Lambda-Edge-GB-Second Identique à l'article correspondant sur votre CloudFront facture.

CloudFront frais figurant sur votre AWS facture	Valeurs figurant dans la UsageType colonne du rapport AWS d'utilisation
KeyValueStore-EdgeReads Le coût du nombre d'appels de lecture aux CloudFront KeyValueStore méthodes`get()`,`exists()`, et`meta()`. Pour plus d'informations, consultez Méthodes d'aide pour les magasins de clés-valeurs.	KeyValueStore-EdgeReads Identique à l'article correspondant sur votre CloudFront facture.
KeyValueStore-APIOperations Le montant correspondant au nombre d'appels à l'CloudFront KeyValueStoreAPI.	KeyValueStore-APIOperations Identique à l'article correspondant sur votre CloudFront facture.

Afficher CloudFront les rapports dans la console

Chaque rapport fournit des informations détaillées et des visualisations, afin que vous puissiez optimiser la diffusion de contenu, identifier les goulets d'étranglement en matière de performance et prendre des décisions fondées sur les données. Que vous ayez besoin de surveiller l'efficacité du cache, d'analyser les modèles de trafic ou de mieux comprendre vos spectateurs, vous pouvez utiliser ces rapports pour surveiller et analyser efficacement vos CloudFront distributions.

Vous pouvez consulter les rapports suivants relatifs à votre CloudFront activité dans la console :

Rubriques

- Afficher les rapports statistiques du CloudFront cache
- Afficher les rapports sur les objets CloudFront populaires
- Afficher les rapports sur CloudFront les meilleurs référents
- Afficher les rapports CloudFront d'utilisation
- Afficher les rapports des CloudFront spectateurs

La plupart de ces rapports sont basés sur les données des journaux CloudFront d'accès, qui contiennent des informations détaillées sur chaque demande d'utilisateur CloudFront reçue. Vous

n’avez pas besoin d’activer les journaux d’accès pour afficher les rapports. Pour plus d’informations, consultez Journaux d'accès (journaux standard).

Afficher les rapports statistiques du CloudFront cache

Le rapport sur les statistiques du CloudFront cache Amazon affiche les informations suivantes :

- Nombre total de demandes : présente le nombre total de demandes pour tous les codes d’état HTTP (par exemple, 200 ou 404) et toutes les méthodes (par exemple, GET, HEAD ou POST)
- Pourcentage de demandes de spectateurs par type de résultat : résultats, échecs et erreurs en pourcentage du total des demandes des spectateurs pour la distribution sélectionnée CloudFront
- Nombre d’octets transférés aux utilisateurs : nombre total d’octets et nombre d’octets des échecs
- Codes d’état HTTP : demandes des utilisateurs par code d’état HTTP
- Pourcentage de demandes GET qui n’ont pas terminé le téléchargement : demandes GET des utilisateurs n’ayant pas terminé le téléchargement de l’objet demandé, en pourcentage du total des demandes

Les données de ces statistiques proviennent de la même source que les journaux CloudFront d'accès. Toutefois, vous n’avez pas besoin d’activer la journalisation des accès pour afficher les statistiques de mise en cache.

Vous pouvez afficher des graphiques pour une plage de dates donnée au cours des 60 derniers jours, avec des points de données chaque heure ou chaque jour. Vous pouvez normalement voir les données sur les requêtes reçues par CloudFront aussi récentes que celle arrivées une heure auparavant, mais elles peuvent parfois être retardées jusqu'à 24 heures.

Rubriques

- Afficher les rapports statistiques du CloudFront cache dans la console
- Téléchargement des données au format CSV
- Comment les graphiques de statistiques de cache sont-ils liés aux données des journaux CloudFront standard (journaux d'accès)

Afficher les rapports statistiques du CloudFront cache dans la console

Vous pouvez consulter le rapport sur les statistiques du CloudFront cache dans la console.

Pour consulter le rapport sur les statistiques du CloudFront cache

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Statistiques de mise en cache.
3. Dans le volet Rapports statistiques de mise en cache CloudFront , pour Start Date (Date de début) et End Date (Date de fin), sélectionnez la période choisie pour l'affichage des graphiques des statistiques de mise en cache. Les plages disponibles dépendent de la valeur sélectionnée pour Granularity (Granularité) :

   - Daily (Quotidien) – Pour afficher les graphiques avec un point de données par jour, sélectionnez n'importe quelle plage de dates au cours des 60 derniers jours.
   - Hourly (Horaire) – Pour afficher les graphiques avec un point de données par heure, sélectionnez une plage de dates de 14 jours maximum au cours des 60 derniers jours.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).
4. Pour Granularity (Granularité), indiquez si vous souhaitez afficher un point de données par jour ou un point de données par heure dans les graphiques. Si vous spécifiez une plage de dates supérieure à 14 jours, il n'est pas possible de spécifier un point de données par heure.
5. Pour Viewer Location (Emplacement de l'utilisateur), choisissez le continent d'où proviennent les requêtes des utilisateurs ou bien All Locations (Tous les emplacements). Les graphiques de statistiques de cache incluent des données pour les demandes CloudFront reçues depuis l'emplacement spécifié.
6. Dans la liste Distribution, sélectionnez les distributions pour lesquelles vous voulez afficher des données dans les graphiques d'utilisation :

   - Une distribution individuelle — Les graphiques affichent les données de la CloudFront distribution sélectionnée. La liste Distribution affiche l'ID de distribution et, le cas échéant, les noms de domaines alternatifs (CNAME) pour la distribution. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste indique les noms de domaines d'origine pour la distribution.
   - Toutes les distributions : les graphiques affichent les données additionnées pour toutes les distributions associées à la distribution actuelle Compte AWS, à l'exception des distributions que vous avez supprimées.
7. Choisissez Mettre à jour.

Tip

- Pour afficher les données associées à un point de données par heure ou par jour, placez le pointeur sur ce point de données.
- Pour les graphiques qui indiquent les données transférées, vous pouvez changer l'échelle verticale afin d'afficher des giga-octets, des méga-octets ou des kilo-octets.

Téléchargement des données au format CSV

Vous pouvez télécharger le rapport de statistiques sur la mise en cache au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport de statistiques sur la mise en cache au format CSV

1. Lorsque le rapport statistique de mise en cache est affiché, choisissez CSV.
2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Granularité

Indique si chaque ligne du rapport représente une heure ou un jour.

ViewerLocation

Le continent duquel proviennent les requêtes des utilisateurs ou ALL, si vous avez choisi de télécharger le rapport pour tous les emplacements.

Données du rapport de statistiques sur la mise en cache

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

ViewerLocation

Le continent duquel proviennent les requêtes des utilisateurs ou ALL, si vous avez choisi de télécharger le rapport pour tous les emplacements.

TimeBucket

Heure du jour auquel les données s'appliquent, en heure UTC.

RequestCount

Le nombre total de requêtes pour tous les codes de statut HTTP (par exemple, 200 ou 404) et toutes les méthodes (par exemple, GET, HEAD ou POST).

HitCount

Le nombre de demandes de visualisation pour lesquelles l'objet est servi à partir d'un cache CloudFront périphérique.

MissCount

Le nombre de requêtes de visualisation pour lesquelles l'objet ne se trouve pas actuellement dans un cache périphérique. Vous CloudFront devez donc obtenir l'objet depuis votre origine.

ErrorCount

Le nombre de requêtes d'utilisateursayant entraîné une erreur, de sorte que CloudFront n'a pas diffusé l'objet.

IncompleteDownloadCount

Le nombre de requêtes d’utilisateursqui ont commencé mais n’ont pas terminé de télécharger l’objet.

HTTP2xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 2xx (réussite).

HTTP3xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 3xx (action supplémentaire exigée).

HTTP4xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 4xx (erreur client).

HTTP5xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 5xx (erreur serveur).

TotalBytes

Nombre total d'octets servis aux spectateurs CloudFront en réponse à toutes les demandes pour toutes les méthodes HTTP.

BytesFromMisses

Nombre d’octets distribués aux utilisateurs pour des objets qui ne se trouvaient pas dans le cache périphérique au moment de la demande. Cette valeur est une bonne approximation des octets transférés depuis votre origine vers les caches CloudFront périphériques. Elle exclut toutefois les requêtes pour des objets se trouvant déjà dans le cache périphérique, mais qui ont expiré.

Comment les graphiques de statistiques de cache sont-ils liés aux données des journaux CloudFront standard (journaux d'accès)

Le tableau suivant montre comment les graphiques de statistiques de cache de la CloudFront console correspondent aux valeurs des journaux CloudFront d'accès. Pour plus d'informations sur les journaux CloudFront d'accès, consultezJournaux d'accès (journaux standard).

Total requests (Nombre total de requêtes)

Ce graphique présente le nombre total de requêtes pour tous les codes de statut HTTP (par exemple, 200 ou 404) et toutes les méthodes (par exemple, `GET`, `HEAD` ou `POST`). Le nombre total de requêtes illustré dans le graphique est égal au nombre total de requêtes dans les fichiers-journaux d'accès sur la même période.

Percentage of Viewer Requests by Result Type (Pourcentage des requêtes d'utilisateurs par type de résultat)

Ce graphique montre les visites, les échecs et les erreurs en pourcentage du total des demandes des spectateurs pour la CloudFront distribution sélectionnée :

- Hit : demande d'utilisateur pour laquelle l'objet est diffusé à partir d'un cache CloudFront périphérique. Dans les journaux d'accès, il s'agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Hit`.
- Absence : requête d'un utilisateur pour laquelle l'objet ne se trouve pas actuellement dans un cache périphérique. CloudFront Vous devez donc récupérer l'objet depuis votre origine. Dans les journaux d'accès, il s'agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Miss`.
- Erreur : requête de l'utilisateur qui a généré une erreur et qui CloudFront n'a donc pas permis de diffuser l'objet. Dans les journaux d'accès, il s'agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Error`, `LimitExceeded` ou `CapacityExceeded`.

Le graphique ne comprend pas les hits actualisés, c'est-à-dire les requêtes pour des objets se trouvant dans le cache périphérique mais ayant expiré. Dans les journaux d'accès, il s'agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `RefreshHit`.

Bytes Transferred to Viewers (Octets transférés aux utilisateurs)

Ce graphique indique deux valeurs :

- Nombre total d'octets : nombre total d'octets servis aux spectateurs CloudFront en réponse à toutes les demandes pour toutes les méthodes HTTP. Dans les journaux CloudFront d'accès,

le nombre total d'octets est la somme des valeurs de la `sc-bytes` colonne pour toutes les demandes au cours de la même période.

- Bytes from Misses (Nombre d’octets provenant d’échecs) – Nombre d’octets servis aux utilisateurs pour des objets qui ne se trouvaient pas dans le cache périphérique au moment de la requête. Dans les journaux CloudFront d'accès, le nombre d'octets perdus est la somme des valeurs de la `sc-bytes` colonne pour les demandes dont la valeur `x-edge-result-type` est est`Miss`. Cette valeur est une bonne approximation des octets transférés depuis votre origine vers les caches CloudFront périphériques. Elle exclut toutefois les requêtes pour des objets se trouvant déjà dans le cache périphérique, mais qui ont expiré.

Codes d’état HTTP

Ce graphique présente les requêtes des utilisateurs par code de statut HTTP. Dans les journaux CloudFront d'accès, les codes d'état apparaissent dans la `sc-status` colonne :

- 2xx – La requête a réussi.
- 3xx – Une action supplémentaire est nécessaire. Par exemple, 301 (Déplacé de façon permanente) signifie que l’objet demandé a été déplacé ailleurs.
- 4xx – Apparemment, le client a fait une erreur. Par exemple, 404 (Non trouvé) signifie que le client a demandé un objet qui est introuvable.
- 5xx – Le serveur d’origine n’a pas satisfait la demande. Par exemple, 503 (Service non disponible) signifie que le serveur d’origine n’est pas disponible actuellement.

Percentage of GET Requests that Didn’t Finish Downloading (Pourcentage de requêtes GET qui n’ont pas terminé le téléchargement)

Ce graphique présente les requêtes d’utilisateurs`GET` qui n’ont pas terminé de télécharger l’objet demandé sous la forme d’un pourcentage du nombre total de requêtes. Généralement, le téléchargement d'un objet ne se termine pas parce que l'utilisateur l'a annulé, par exemple en choisissant un autre lien ou en fermant le navigateur. Dans les journaux CloudFront d'accès, ces demandes ont une valeur de `200` dans la `sc-status` colonne et une valeur de `Error` dans la `x-edge-result-type` colonne.

Afficher les rapports sur les objets CloudFront populaires

Consultez le rapport Amazon CloudFront Popular Objects pour voir les 50 objets les plus populaires pour une distribution au cours d'une période spécifiée au cours des 60 derniers jours. Vous pouvez également afficher des statistiques sur ces objets, notamment les suivantes :

- Nombre de demandes pour l’objet
- Nombre de résultats et d’échecs
- Hit Ratio (proportion de résultats)
- Nombre d’octets servis en cas d’échec
- Nombre total d’octets servis
- Nombre de téléchargements incomplets
- Nombre de demandes par code d’état HTTP (2xx, 3xx, 4xx et 5xx)

Les données de ces statistiques proviennent de la même source que les journaux CloudFront d'accès. Toutefois, vous n’avez pas besoin d’activer la journalisation des accès pour afficher les objets populaires.

Rubriques

- Afficher CloudFront les rapports sur les objets populaires dans la console
- Comment CloudFront calcule les statistiques des objets populaires
- Téléchargement des données au format CSV
- Comment les données du rapport sur les objets populaires sont liées aux données des journaux CloudFront standard (journaux d'accès)

Afficher CloudFront les rapports sur les objets populaires dans la console

Vous pouvez consulter le rapport sur les objets CloudFront populaires dans la console.

Pour afficher les objets populaires d'une CloudFront distribution

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Objets populaires.
3. Dans le volet CloudFront Popular Objects Report (Rapport d'objets populaires), pour Start Date (Date de début) et End Date (Date de fin), sélectionnez la période d'affichage de la liste des objets populaires. Vous pouvez choisir n’importe quelle période comprise dans les 60 jours qui précèdent.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).

4. Dans la liste Distribution (Distribution), sélectionnez la distribution pour laquelle vous voulez afficher une liste des objets populaires.
5. Choisissez Mettre à jour.

Comment CloudFront calcule les statistiques des objets populaires

Pour obtenir un décompte précis des 50 principaux objets de votre distribution, CloudFront comptez les demandes pour tous vos objets à des intervalles de 10 minutes à partir de minuit et conservez un total cumulé des 150 meilleurs objets pour les 24 prochaines heures. (conserve CloudFront également les totaux quotidiens des 150 meilleurs objets pendant 60 jours.)

Comme les objets du bas de la liste s'élèvent ou disparaissent continuellement, leurs totaux sont approximatifs. La position des 50 objets du haut de la liste de 150 éléments peut varier, mais ils disparaissent rarement de la liste. Les totaux correspondants sont donc normalement plus fiables.

Lorsqu'un objet sort de la liste des 150 premiers objets, puis y remonte au cours d'une journée, CloudFront ajoute un nombre estimé de demandes pour la période pendant laquelle l'objet était absent de la liste. Cette estimation est basée sur le nombre de requêtes reçues par le dernier objet de la liste pendant cette période.

Si l'objet se classe parmi les 50 premiers objets plus tard dans la journée, les estimations du nombre de demandes CloudFront reçues alors que l'objet figurait parmi les 150 premiers objets font généralement en sorte que le nombre de demandes figurant dans le rapport sur les objets les plus populaires dépasse le nombre de demandes qui apparaissent dans les journaux d'accès pour cet objet.

Téléchargement des données au format CSV

Vous pouvez télécharger le rapport des objets populaires au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport des objets populaires au format CSV

1. Pendant que le rapport des objets populaires est affiché, choisissez CSV.
2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Données du rapport des objets populaires

Le rapport inclut les valeurs suivantes :

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Objet

Les 500 derniers caractères de l'URL de l'objet.

RequestCount

Le nombre total de requêtes pour cet objet.

HitCount

Le nombre de demandes de visualisation pour lesquelles l'objet est servi à partir d'un cache CloudFront périphérique.

MissCount

Le nombre de requêtes de visualisation pour lesquelles l'objet ne se trouve pas actuellement dans un cache périphérique. Vous CloudFront devez donc obtenir l'objet depuis votre origine.

HitCountPct

La valeur de `HitCount` en pourcentage de la valeur de `RequestCount`.

BytesFromMisses

Nombre d’octets distribués aux utilisateurs pour cet objet alors que l’objet ne se trouvait pas dans le cache périphérique au moment de la demande.

TotalBytes

Nombre total d'octets servis aux spectateurs par CloudFront cet objet en réponse à toutes les requêtes pour toutes les méthodes HTTP.

IncompleteDownloadCount

Le nombre de requêtes pour cet objet que les utilisateurs ont lancé sans terminer de télécharger l’objet.

HTTP2xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 2xx (réussite).

HTTP3xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 3xx (action supplémentaire exigée).

HTTP4xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 4xx (erreur client).

HTTP5xx

Le nombre de requêtes d’utilisateurspour lesquelles le code de statut HTTP était de type 5xx (erreur serveur).

Comment les données du rapport sur les objets populaires sont liées aux données des journaux CloudFront standard (journaux d'accès)

La liste suivante montre comment les valeurs du rapport des objets populaires de la CloudFront console correspondent aux valeurs des journaux CloudFront d'accès. Pour plus d'informations sur les journaux d'accès CloudFront, consultez Journaux d'accès (journaux standard).

URL

Les 500 derniers caractères de l'URL employée par les utilisateurs pour accéder à l'objet.

Requêtes

Le nombre total de requêtes pour l'objet. Cette valeur correspond généralement étroitement au nombre de `GET` requêtes pour l'objet dans les journaux CloudFront d'accès.

Hits

Le nombre de requêtes d'utilisateurspour lesquelles l'objet a été diffusé à partir d'un cache périphérique CloudFront . Dans les journaux d'accès, il s'agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Hit`.

Miss

Le nombre de requêtes des utilisateurs pour lesquelles l'objet ne se trouvait pas dans un cache périphérique. Vous avez donc CloudFront récupéré l'objet depuis votre origine. Dans les journaux d'accès, il s'agit des requêtes pour lesquelles `x-edge-response-result-type` a une valeur de `Miss`.

Hit Ratio (proportion de résultats)

Valeur de la colonne Hits (Hits) en tant que pourcentage de la valeur de la colonne Requests (Requêtes).

Bytes from Misses (Octets provenant d'échecs)

Nombre d'octets distribués aux utilisateurs pour des objets qui ne se trouvaient pas dans le cache périphérique au moment de la demande. Dans les journaux CloudFront d'accès, le nombre d'octets perdus est la somme des valeurs de la `sc-bytes` colonne pour les demandes dont la valeur `x-edge-result-type` est est`Miss`.

Total Bytes (Nombre total d'octets)

Nombre total d'octets qui CloudFront ont été transmis aux spectateurs en réponse à toutes les demandes concernant l'objet pour toutes les méthodes HTTP. Dans les journaux CloudFront

d'accès, le nombre total d'octets est la somme des valeurs de la `sc-bytes` colonne pour toutes les demandes au cours de la même période.

Incomplete Downloads (Téléchargements incomplets)

Le nombre de requêtes d’utilisateursqui n’ont pas terminé de téléchargé l’objet demandé. Généralement, un téléchargement ne se termine pas parce que l'utilisateur l'a annulé, par exemple en choisissant un autre lien ou en fermant le navigateur. Dans les journaux CloudFront d'accès, ces demandes ont une valeur de `200` dans la `sc-status` colonne et une valeur de `Error` dans la `x-edge-result-type` colonne.

2xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est `2xx`, `Successful`. Dans les journaux CloudFront d'accès, les codes d'état apparaissent dans la `sc-status` colonne.

3xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est de type `3xx`, `Redirection`. Le code de statut de type `3xx` indique qu’une action supplémentaire est exigée. Par exemple, 301 (Déplacé de façon permanente) signifie que l’objet demandé a été déplacé ailleurs.

4xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est de type `4xx`, `Client Error`. Le code de statut de type `4xx` indique que le client aurait fait une erreur. Par exemple, 404 (Non trouvé) signifie que le client a demandé un objet qui est introuvable.

5xx

Le nombre de requêtes pour lesquelles le code de statut HTTP est de type `5xx`, `Server Error`. Le code de statut de type `5xx` indique que le serveur d’origine n’a pas satisfait la demande. Par exemple, 503 (Service non disponible) signifie que le serveur d’origine n’est pas disponible actuellement.

Afficher les rapports sur CloudFront les meilleurs référents

Le rapport sur les CloudFront principaux référents inclut les informations suivantes pour n'importe quelle plage de dates au cours des 60 derniers jours :

- Les 25 principaux référents (domaines des sites Web qui ont généré le plus de requêtes HTTP et HTTPS pour les objets CloudFront distribués pour votre distribution)
- Nombre de demandes d’un référent

- Le nombre de demandes envoyées par un référent sous forme de pourcentage du nombre total de demandes au cours de la période spécifiée

Les données du rapport sur les principaux référents proviennent de la même source que les journaux CloudFront d'accès. Cependant, vous n'avez pas besoin d'activer la journalisation des accès pour afficher les principaux référents.

Les principaux référents peuvent être des moteurs de recherche, d'autres sites web contenant des liens directs vers vos objets ou encore votre propre site. Par exemple, si `https://example.com/index.html` contient des liens vers 10 éléments graphiques, `example.com` est le référent pour ces 10 éléments.

> **Note**
>
> Si un utilisateur saisit une URL directement dans la ligne d'adresse d'un navigateur, il n'existe pas de référent pour l'objet demandé.

Rubriques

- Afficher les rapports sur les CloudFront principaux référents dans la console
- Comment CloudFront calcule les statistiques des meilleurs référents
- Téléchargement des données au format CSV
- Comment les données du rapport des principaux référents sont liées aux données des journaux CloudFront standard (journaux d'accès)

Afficher les rapports sur les CloudFront principaux référents dans la console

Vous pouvez consulter le rapport sur les CloudFront principaux référents dans la console.

Pour afficher les principaux référents d'une distribution CloudFront

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Principaux référents.
3. Dans le volet Rapport CloudFront sur les principaux référents, pour Start Date (Date de début) et End Date (Date de fin), sélectionnez la période pour laquelle vous souhaitez afficher la liste des principaux référents.

Les dates et heures sont exprimées en heure UTC (temps universel coordonné).

4. Dans la liste Distribution (Distribution), sélectionnez la distribution pour laquelle vous voulez afficher une liste des principaux référents.
5. Choisissez Mettre à jour.

Comment CloudFront calcule les statistiques des meilleurs référents

Pour obtenir un décompte précis des 25 principaux référents, CloudFront comptez les demandes pour tous vos objets à des intervalles de 10 minutes et conservez le total cumulé des 75 meilleurs référents. Comme les référents du bas de la liste s'élèvent ou disparaissent continuellement, leurs totaux sont approximatifs.

La position des 25 référents du haut de la liste de 75 éléments peut varier, mais ils disparaissent rarement de la liste. Les totaux correspondants sont donc normalement plus fiables.

Téléchargement des données au format CSV

Vous pouvez télécharger le rapport sur les principaux référents au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport sur les principaux référents au format CSV

1. Alors que le rapport des principaux référents est affiché, choisissez CSV.
2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Données du rapport sur les principaux référents

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou ALL si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Referrer

Le nom de domaine du référent.

RequestCount

Le nombre total de requêtes en provenance du nom de domaine de la colonne `Referrer`.

RequestsPct

Le nombre de requêtes envoyées par le référent sous forme de pourcentage du nombre total de requêtes au cours de la période spécifiée.

Comment les données du rapport des principaux référents sont liées aux données des journaux CloudFront standard (journaux d'accès)

La liste suivante montre comment les valeurs du rapport Top Referrers de la CloudFront console correspondent aux valeurs des journaux d' CloudFront accès. Pour plus d'informations sur les journaux d'accès CloudFront, consultez Journaux d'accès (journaux standard).

Referrer

Le nom de domaine du référent. Dans les journaux d’accès, les référents figurent dans la colonne `cs(Referer)`.

Request Count

Le nombre total de requêtes en provenance du nom de domaine de la colonne Référent. Cette valeur correspond généralement étroitement au nombre de `GET` requêtes du référent dans les journaux CloudFront d'accès.

Requête %

Le nombre de requêtes envoyées par le référent sous forme de pourcentage du nombre total de requêtes au cours de la période spécifiée. Si vous avez plus de 25 référents, vous ne pouvez pas calculer Request % (Requête %) sur la base des données de ce tableau, car la colonne Request Count (Nombre de requêtes) n’inclut pas toutes les requêtes pendant la période spécifiée.

Afficher les rapports CloudFront d'utilisation

Les rapports CloudFront d'utilisation contiennent les informations suivantes :

- Nombre de demandes : affiche le nombre total de demandes auxquelles il est CloudFront répondu depuis des emplacements périphériques de la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée.
- Données transférées par protocole et données transférées par destination : les deux indiquent la quantité totale de données transférées depuis des emplacements CloudFront périphériques de la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée. Les données sont séparées différemment, comme suit :
  - By protocol (Par protocole) — Sépare les données par protocole : HTTP ou HTTPS.
  - Par destination : sépare les données par destination : à vos utilisateurs ou votre origine.

Le rapport CloudFront d'utilisation est basé sur le rapport AWS d'utilisation de CloudFront. Ce rapport ne nécessite aucune configuration supplémentaire. Pour plus d'informations, consultez Consultez le AWS rapport d'utilisation pour CloudFront.

Vous pouvez afficher des rapports pour une période donnée au cours des 60 derniers jours, avec des points de données chaque heure ou chaque jour. Vous pouvez généralement consulter les données relatives aux demandes CloudFront reçues il y a à peine quatre heures, mais les données peuvent parfois être retardées de 24 heures.

Pour plus d'informations, consultez Comment les graphiques d'utilisation sont-ils liés aux données du rapport CloudFront d'utilisation ?.

Rubriques

- Afficher les rapports CloudFront d'utilisation dans la console
- Téléchargement des données au format CSV
- Comment les graphiques d'utilisation sont-ils liés aux données du rapport CloudFront d'utilisation ?

Afficher les rapports CloudFront d'utilisation dans la console

Vous pouvez consulter le rapport CloudFront d'utilisation dans la console.

Pour consulter les rapports CloudFront d'utilisation

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation, choisissez Rapports d'utilisation.
3. Dans le volet Rapports d'utilisation de CloudFront , pour Start Date (Date de début) et End Date (Date de fin), sélectionnez la période pour laquelle vous souhaitez afficher les graphiques d'utilisation. Les plages disponibles dépendent de la valeur sélectionnée pour Granularity (Granularité) :

   - Daily (Quotidien) – Pour afficher les graphiques avec un point de données par jour, sélectionnez n'importe quelle plage de dates au cours des 60 derniers jours.
   - Hourly (Horaire) – Pour afficher les graphiques avec un point de données par heure, sélectionnez une plage de dates de 14 jours maximum au cours des 60 derniers jours.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).

4. Pour Granularity (Granularité), indiquez si vous souhaitez afficher un point de données par jour ou un point de données par heure dans les graphiques. Si vous spécifiez une plage de dates supérieure à 14 jours, il n'est pas possible de spécifier un point de données par heure.
5. Pour la région de facturation, choisissez la région CloudFront de facturation qui contient les données que vous souhaitez consulter, ou choisissez Toutes les régions. Les graphiques d'utilisation incluent les données des requêtes traitées par CloudFront dans les emplacements périphériques de la région spécifiée. La région dans laquelle CloudFront les demandes sont traitées peut ne pas correspondre à la localisation de vos spectateurs.

   Sélectionnez uniquement les régions incluses dans la catégorie tarifaire de votre distribution. Dans le cas contraire, les graphiques d'utilisation ne contiendront probablement aucune donnée. Par exemple, si vous avez choisi la classe de prix 200 pour votre distribution, les régions de facturation d'Amérique du Sud et d'Australie ne sont pas incluses. Nous ne traiterons donc CloudFront généralement pas vos demandes provenant de ces régions. Pour plus d'informations sur les classes de prix, consultez la section CloudFront Tarification.
6. Dans la liste Distribution, sélectionnez les distributions pour lesquelles vous voulez afficher des données dans les graphiques d'utilisation :

   - Une distribution individuelle — Les graphiques affichent les données de la CloudFront distribution sélectionnée. La liste Distribution affiche l'ID de distribution et, le cas échéant, les noms de domaines alternatifs (CNAME) pour la distribution. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste indique les noms de domaines d'origine pour la distribution.
   - Toutes les distributions (exclues les distributions supprimées) — Les graphiques affichent les données cumulées pour toutes les distributions associées au AWS compte courant, à l'exception des distributions que vous avez supprimées.
   - Toutes les distributions supprimées — Les graphiques affichent les données cumulées pour toutes les distributions associées au AWS compte courant et qui ont été supprimées au cours des 60 derniers jours.
7. Choisissez Mettre à jour les graphiques.

> **Tip**
>
> - Pour afficher les données associées à un point de données par heure ou par jour, placez le pointeur sur ce point de données.

- Pour les graphiques qui indiquent les données transférées, notez bien que vous pouvez changer l'échelle verticale afin d'afficher des giga-octets, des méga-octets ou des kilo-octets.

Téléchargement des données au format CSV

Vous pouvez télécharger le rapport d'utilisation au format CSV. Cette section explique comment télécharger le rapport et décrire les valeurs du rapport.

Pour télécharger le rapport d'utilisation au format CSV

1. Alors que le rapport d'utilisation est affiché, choisissez CSV.
2. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport, `ALL` si le rapport concernait toutes les distributions, ou `ALL_DELETED` si le rapport concernait toutes les distributions supprimées.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Granularité

Indique si chaque ligne du rapport représente une heure ou un jour.

BillingRegion

Le continent duquel proviennent les requêtes des utilisateurs ou `ALL`, si vous avez choisi de télécharger le rapport pour toutes les régions de facturation.

Données du rapport d'utilisation

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport, `ALL` si le rapport concernait toutes les distributions, ou `ALL_DELETED` si le rapport concernait toutes les distributions supprimées.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

BillingRegion

La région CloudFront de facturation pour laquelle vous avez généré le rapport, ou`ALL`.

TimeBucket

Heure du jour auquel les données s'appliquent, en heure UTC.

HTTP

Le nombre de requêtes HTTP auxquelles CloudFront ont répondu des localisations périphériques de la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Le nombre de `HEAD` demandes `GET` et le nombre de demandes qui CloudFront entraînent le transfert de données à vos spectateurs
- Le nombre de`DELETE`,, `OPTIONS` `PATCH``POST`, et de `PUT` demandes qui entraînent le transfert CloudFront de données vers votre lieu d'origine

HTTPS

Le nombre de requêtes HTTPS auxquelles CloudFront ont répondu des localisations périphériques de la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Le nombre de HEAD demandes GET et le nombre de demandes qui CloudFront entraînent le transfert de données à vos spectateurs
- Le nombre deDELETE,, OPTIONS PATCHPOST, et de PUT demandes qui entraînent le transfert CloudFront de données vers votre lieu d'origine

HTTPBytes

La quantité totale de données transférées via HTTP depuis des emplacements CloudFront périphériques dans la région de facturation sélectionnée au cours de la période de CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Données transférées de CloudFront à vos spectateurs en réponse à GET des HEAD demandes
- Données transférées par vos spectateurs vers CloudFront les formulairesDELETE,OPTIONS, PATCHPOST, et les PUT requêtes
- Données transférées de CloudFront à vos spectateurs en réponse àDELETE,OPTIONS, PATCHPOST, et PUT aux demandes

HTTPSBytes

La quantité totale de données transférées via HTTPS depuis des emplacements CloudFront périphériques dans la région de facturation sélectionnée au cours de la période de CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Données transférées de CloudFront à vos spectateurs en réponse à GET des HEAD demandes
- Données transférées par vos spectateurs vers CloudFront les formulairesDELETE,OPTIONS, PATCHPOST, et les PUT requêtes
- Données transférées de CloudFront à vos spectateurs en réponse àDELETE,OPTIONS, PATCHPOST, et PUT aux demandes

BytesIn

La quantité totale de données transférées depuis votre CloudFront lieu d'origine pourDELETE,, OPTIONS PATCHPOST, et les PUT demandes dans la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée.

BytesOut

La quantité totale de données transférées via HTTP et HTTPS CloudFront vers vos spectateurs dans la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée. Les valeurs sont les suivantes :

- Données transférées de CloudFront à vos spectateurs en réponse à `GET` des `HEAD` demandes
- Données transférées de CloudFront à vos spectateurs en réponse à`DELETE`,`OPTIONS`, `PATCH`POST, et `PUT` aux demandes

Comment les graphiques d'utilisation sont-ils liés aux données du rapport CloudFront d'utilisation ?

La liste suivante montre comment les graphiques d'utilisation de la CloudFront console correspondent aux valeurs de la colonne Type d'utilisation du rapport CloudFront d'utilisation.

Rubriques

- Nombre de demandes
- Données transférées par protocole
- Données transférées par destination

Nombre de demandes

Ce graphique montre le nombre total de demandes auxquelles il CloudFront est répondu depuis des emplacements périphériques de la région sélectionnée pendant chaque intervalle de temps pour la CloudFront distribution spécifiée, en les séparant par protocole (HTTP ou HTTPS) et type (statique, dynamique ou proxy).

Nombre de requêtes HTTP

- *`region`*- Requests-HTTP-Static : Nombre de requêtes HTTP `GET` et de `HEAD` requêtes traitées pour des objets dont le TTL est supérieur ou égal à 3600 secondes
- *`region`*- Requests-HTTP-Dynamic : Nombre de requêtes HTTP `GET` et de `HEAD` requêtes traitées pour des objets dont le TTL est inférieur à 3600 secondes
- *`region`*- Requests-HTTP-Proxy : Nombre de `PUT` requêtes HTTP`DELETE`,`OPTIONS`, `PATCH`POST, et qui sont redirigées CloudFront vers votre point d'origine

Nombre de requêtes HTTPS

- *region*- Requests-HTTPS-Static : Nombre de HEAD requêtes HTTPS GET et traitées pour des objets dont le TTL est supérieur ou égal à 3600 secondes
- *region*- Requests-HTTPS-Dynamic : Nombre de HEAD requêtes HTTPS GET et traitées pour des objets dont le TTL est inférieur à 3600 secondes
- *region*- Requests-HTTPS-Proxy : Nombre de PUT requêtes HTTPSDELETE,OPTIONS, PATCHPOST, et qui sont redirigées CloudFront vers votre point d'origine

Données transférées par protocole

Ce graphique montre la quantité totale de données transférées depuis des emplacements CloudFront périphériques de la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée, en les séparant par protocole (HTTP ou HTTPS), type (statique, dynamique ou proxy) et destination (spectateurs ou origine).

Données transférées par HTTP

- *region*- Out-Bytes-HTTP-Static : Octets servis en utilisant le protocole HTTP pour les objets dont le TTL est supérieur ou égal à 3600 secondes
- *region*- Out-Bytes-HTTP-Dynamic : Octets servis en utilisant le protocole HTTP pour les objets dont le TTL est inférieur à 3600 secondes
- *region*- Out-Bytes-HTTP-Proxy : octets renvoyés par CloudFront les spectateurs en utilisant HTTP en réponse aux PUT requêtes DELETE OPTIONS PATCHPOST,, et
- *region*- Out-OBytes-HTTP-Proxy : Nombre total d'octets transférés via HTTP depuis les emplacements CloudFront périphériques vers votre origine en réponse à DELETEOPTIONS, PATCHPOST, et PUT aux requêtes

Données transférées par HTTPS

- *region*- Out-Bytes-HTTPS-Static : Octets servis en utilisant le protocole HTTPS pour les objets dont le TTL est supérieur ou égal à 3600 secondes
- *region*- Out-Bytes-HTTPS-Dynamic : Octets servis en utilisant le protocole HTTPS pour les objets dont le TTL est inférieur à 3600 secondes
- *region*- Out-Bytes-HTTPS-Proxy : octets renvoyés par les spectateurs CloudFront à l'aide du protocole HTTPS en réponse aux PUT requêtes DELETE OPTIONS PATCHPOST,, et

- *region*- Out-OBytes-HTTPS-Proxy : Nombre total d'octets transférés à l'aide du protocole HTTPS depuis les emplacements CloudFront périphériques vers votre origine en réponse à DELETE OPTIONSPATCH,POST, et PUT aux requêtes

Données transférées par destination

Ce graphique montre la quantité totale de données transférées depuis des emplacements CloudFront périphériques de la région sélectionnée au cours de chaque intervalle de temps pour la CloudFront distribution spécifiée, en les séparant par destination (spectateurs ou origine), protocole (HTTP ou HTTPS) et type (statique, dynamique ou proxy).

Données transférées de CloudFront à vos spectateurs

- *region*- Out-Bytes-HTTP-Static : Octets servis en utilisant le protocole HTTP pour les objets dont le TTL est supérieur ou égal à 3600 secondes
- *region*- Out-Bytes-HTTPS-Static : Octets servis en utilisant le protocole HTTPS pour les objets dont le TTL est supérieur ou égal à 3600 secondes
- *region*- Out-Bytes-HTTP-Dynamic : Octets servis en utilisant le protocole HTTP pour les objets dont le TTL est inférieur à 3600 secondes
- *region*- Out-Bytes-HTTPS-Dynamic : Octets servis en utilisant le protocole HTTPS pour les objets dont le TTL est inférieur à 3600 secondes
- *region*- Out-Bytes-HTTP-Proxy : octets renvoyés par CloudFront les spectateurs en utilisant HTTP en réponse aux PUT requêtes DELETE OPTIONS PATCHPOST,, et
- *region*- Out-Bytes-HTTPS-Proxy : octets renvoyés par les spectateurs CloudFront à l'aide du protocole HTTPS en réponse aux PUT requêtes DELETE OPTIONS PATCHPOST,, et

Données transférées depuis votre CloudFront lieu d'origine

- *region*- Out-OBytes-HTTP-Proxy : Nombre total d'octets transférés via HTTP depuis les emplacements CloudFront périphériques vers votre origine en réponse à DELETEOPTIONS, PATCHPOST, et PUT aux requêtes
- *region*- Out-OBytes-HTTPS-Proxy : Nombre total d'octets transférés à l'aide du protocole HTTPS depuis les emplacements CloudFront périphériques vers votre origine en réponse à DELETE OPTIONSPATCH,POST, et PUT aux requêtes

Afficher les rapports des CloudFront spectateurs

CloudFront Les rapports des spectateurs incluent les informations suivantes pour n'importe quelle plage de dates au cours des 60 derniers jours :

- Appareils : les types d'appareils les plus fréquemment utilisés pour accéder à votre contenu (tels que les ordinateurs de bureau ou les appareils mobiles)
- Navigateurs : les 10 navigateurs les plus fréquemment utilisés pour accéder à votre contenu (tels que Chrome ou Firefox)
- Systèmes d'exploitation : les 10 systèmes d'exploitation les plus fréquemment utilisés pour accéder à votre contenu (tels que Linux, macOS ou Windows)
- Emplacements — Les 50 meilleurs sites (pays ou U.S. states/territories) des spectateurs qui accèdent le plus fréquemment à votre contenu
  - Vous pouvez également afficher les emplacements avec des points de données horaires pour n'importe quelle période allant jusqu'à 14 jours au cours des 60 derniers jours

> **Note**
>
> Vous n'avez pas besoin d'activer la journalisation des accès pour afficher les graphiques et rapports sur les utilisateurs.

Rubriques

- Consultation des graphiques et des rapports sur les utilisateurs dans la console
- Téléchargement des données au format CSV
- Données incluses dans les rapports sur les utilisateurs
- Comment les données du rapport de localisation sont-elles liées aux données des journaux CloudFront standard (journaux d'accès)

Consultation des graphiques et des rapports sur les utilisateurs dans la console

Vous pouvez consulter CloudFront les graphiques et les rapports des spectateurs dans la console.

Pour consulter les graphiques et les rapports des CloudFront spectateurs

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Utilisateurs.
3. Dans le volet Utilisateurs de CloudFront , pour Start Date (Date de début) et End Date (Date de fin), sélectionnez la période pour laquelle vous souhaitez afficher des graphiques et rapports d'utilisateurs.

   Pour le graphique Locations (Emplacements), les plages disponibles dépendent de la valeur sélectionnée pour Granularity (Granularité) :

   - Daily (Quotidien) – Pour afficher les graphiques avec un point de données par jour, sélectionnez n’importe quelle plage de dates au cours des 60 derniers jours.
   - Hourly (Horaire) – Pour afficher les graphiques avec un point de données par heure, sélectionnez une plage de dates de 14 jours maximum au cours des 60 derniers jours.

   Les dates et heures sont exprimées en heure UTC (temps universel coordonné).
4. (Graphiques Browsers (Navigateurs) et Operating Systems (Systèmes d’exploitation) uniquement) Pour Grouping (Groupement), indiquez si vous souhaitez regrouper les navigateurs et systèmes d’exploitation par nom (Chrome, Firefox) ou par nom et version (Chrome 40.0, Firefox 35.0).
5. (Graphique Locations (Emplacements) uniquement) Pour Granularity (Granularité), indiquez si vous souhaitez afficher un point de données par jour ou un point de données par heure dans les graphiques. Si vous spécifiez une plage de dates supérieure à 14 jours, il n’est pas possible de spécifier un point de données par heure.
6. (Tableau des emplacements uniquement) Pour plus de détails, indiquez si vous souhaitez afficher les principales localisations par pays ou par État U.S.
7. Dans la liste Distribution (Distribution), sélectionnez la distribution pour laquelle vous souhaitez afficher des données dans les graphiques d’utilisation :

   - Une distribution individuelle — Les graphiques affichent les données de la CloudFront distribution sélectionnée. La liste Distribution (Distribution) affiche l’ID de distribution et, le cas échéant, un nom de domaine alternatif (CNAME) pour la distribution. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d’origine pour la distribution.

- Toutes les distributions (excepté celles supprimées) – les graphiques affichent le total des données de toutes les distributions qui sont associées au compte AWS actuel, à l'exception des distributions que vous avez supprimées.

8. Choisissez Mettre à jour.

Pour afficher les données associées à un point de données par heure ou par jour, placez le pointeur sur ce point de données.

Téléchargement des données au format CSV

Vous pouvez télécharger chacun des rapports sur les utilisateurs au format CSV. Cette section explique comment télécharger les rapports et décrit les valeurs des rapports.

Pour télécharger les rapports sur les utilisateurs au format CSV

1. Lorsque vous consultez le rapport sur les utilisateurs, choisissez CSV.
2. Choisissez les données à télécharger, par exemple Devices (Appareils) ou Devices Trends (Tendances des appareils).
3. Dans la boîte de dialogue Opening nom de fichier, indiquez si vous souhaitez ouvrir ou enregistrer le fichier.

Données incluses dans les rapports sur les utilisateurs

Les premières lignes de chaque rapport comportent les informations suivantes :

Version

La version du format de ce fichier CSV.

Rapport

Nom du rapport.

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Regroupement (rapports sur les navigateurs et les systèmes d'exploitation uniquement)

Groupement des données par nom ou par nom et version des navigateurs et systèmes d'exploitation.

Granularité

Indique si chaque ligne du rapport représente une heure ou un jour.

Détails (rapport sur les emplacements uniquement)

Indique si les demandes sont répertoriées par pays ou par État U.S.

Les rubriques suivantes décrivent les informations contenues dans les différents rapports sur les utilisateurs.

Rubriques

- Rapport sur les périphériques
- Rapport sur les tendances des périphériques
- Rapport sur les navigateurs
- Rapport sur les tendances des navigateurs
- Rapport sur les systèmes d'exploitation
- Rapport sur les tendances des systèmes d'exploitation
- Rapport sur les emplacements
- Rapport sur les tendances des emplacements

Rapport sur les périphériques

Le rapport inclut les valeurs suivantes :

DistributionID

L’ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d’origine pour la distribution.

Requêtes

Le nombre de demandes CloudFront reçues de chaque type d'appareil.

RequestsPct

Le nombre de demandes CloudFront reçues de chaque type d'appareil en pourcentage du nombre total de demandes CloudFront reçues de tous les appareils.

Personnalisé

Requêtes pour lesquelles la valeur de l’en-tête HTTP `User-Agent` n’a pas été associée à l’un des types d’appareils standard, par exemple `Desktop` ou `Mobile`.

Rapport sur les tendances des périphériques

Le rapport inclut les valeurs suivantes :

DistributionID

L’ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d’origine pour la distribution.

TimeBucket

L’heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

Desktop

Le nombre de demandes CloudFront reçues depuis des ordinateurs de bureau au cours de la période.

Applications mobiles

Le nombre de demandes CloudFront reçues depuis des appareils mobiles au cours de la période. Les appareils mobiles peuvent inclure les tablettes et les téléphones portables. S'il n'est pas CloudFront possible de déterminer si une demande provient d'un appareil mobile ou d'une tablette, elle est comptabilisée dans la `Mobile` colonne.

Smart-TV

Le nombre de demandes CloudFront reçues de téléviseurs intelligents au cours de la période.

Tablet

Le nombre de demandes CloudFront reçues depuis des tablettes au cours de la période. S'il n'est pas CloudFront possible de déterminer si une demande provient d'un appareil mobile ou d'une tablette, elle est comptabilisée dans la `Mobile` colonne.

Je ne sais pas

Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` n'a pas été associée à l'un des types d'appareils standard, par exemple `Desktop` ou `Mobile`.

Empty

Le nombre de demandes CloudFront reçues qui n'incluaient pas de valeur dans l'`User-Agent`en-tête HTTP au cours de la période.

Rapport sur les navigateurs

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Groupe

Le navigateur ou le navigateur et la version qui CloudFront ont reçu les demandes, en fonction de la valeur de`Grouping`. En plus des noms de navigateur, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler— principalement les demandes des moteurs de recherche qui indexent votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` était vide.
- Autres : navigateurs CloudFront identifiés mais qui ne figurent pas parmi les plus populaires. Si`Bot/Crawler`,`Empty`, and/or `Unknown` n'apparaît pas parmi les neuf premières valeurs, elles sont également incluses`Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` n'a pas été associée à un navigateur standard. La plupart des requêtes de cette catégorie proviennent d'applications ou de scripts personnalisés.

Requêtes

Le nombre de demandes CloudFront reçues de chaque type de navigateur.

RequestsPct

Le nombre de demandes CloudFront reçues de chaque type de navigateur en pourcentage du nombre total de demandes CloudFront reçues au cours de la période.

Rapport sur les tendances des navigateurs

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

(Browsers)

Les colonnes restantes du rapport répertorient les navigateurs ou les navigateurs et versions, en fonction de la valeur de `Grouping`. En plus des noms de navigateur, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler— principalement les demandes des moteurs de recherche qui indexent votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` était vide.
- Autres : navigateurs CloudFront identifiés mais qui ne figurent pas parmi les plus populaires. Si`Bot/Crawler`,`Empty`, and/or `Unknown` n'apparaît pas parmi les neuf premières valeurs, elles sont également incluses`Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` n'a pas été associée à un navigateur standard. La plupart des requêtes de cette catégorie proviennent d'applications ou de scripts personnalisés.

Rapport sur les systèmes d'exploitation

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

Groupe

Le système d'exploitation ou le système d'exploitation et sa version ayant envoyé des requêtes à CloudFront, en fonction de la valeur de `Grouping`. En plus des noms de systèmes d’exploitation, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler— principalement les demandes des moteurs de recherche qui indexent votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l’en-tête HTTP `User-Agent` était vide.
- Autres : systèmes d'exploitation CloudFront identifiés mais qui ne figurent pas parmi les plus populaires. Si`Bot/Crawler`,`Empty`, and/or `Unknown` n'apparaît pas parmi les neuf premières valeurs, elles sont également incluses`Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles la valeur de l’en-tête HTTP `User-Agent` n’a pas été associée à un navigateur standard. La plupart des requêtes de cette catégorie proviennent d’applications ou de scripts personnalisés.

Requêtes

Le nombre de demandes CloudFront reçues de chaque type de système d'exploitation.

RequestsPct

Le nombre de demandes CloudFront reçues de chaque type de système d'exploitation en pourcentage du nombre total de demandes CloudFront reçues au cours de la période.

Rapport sur les tendances des systèmes d’exploitation

Le rapport inclut les valeurs suivantes :

DistributionID

L’ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d’origine pour la distribution.

TimeBucket

L’heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

(Operating systems)

Les colonnes restantes du rapport répertorient les systèmes d'exploitation ou les systèmes d'exploitation et versions, en fonction de la valeur de `Grouping`. En plus des noms de systèmes d'exploitation, les paramètres possibles incluent les valeurs suivantes :

- Bot/Crawler— principalement les demandes des moteurs de recherche qui indexent votre contenu.
- Empty (Vide) – Requêtes pour lesquelles la valeur de l'en-tête HTTP `User-Agent` était vide.
- Autres : systèmes d'exploitation CloudFront identifiés mais qui ne figurent pas parmi les plus populaires. Si`Bot/Crawler`,`Empty`, and/or `Unknown` n'apparaît pas parmi les neuf premières valeurs, elles sont également incluses`Other`.
- Unknown (Inconnu) – Requêtes pour lesquelles le système d'exploitation n'est pas spécifié dans l'en-tête HTTP `User-Agent`.

Rapport sur les emplacements

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

LocationCode

Abréviation de l'emplacement qui CloudFront a reçu les demandes. Pour plus d'informations sur les valeurs possibles, consultez la description de Location dans Comment les données du rapport de localisation sont-elles liées aux données des journaux CloudFront standard (journaux d'accès).

LocationName

Nom de l'emplacement en provenance duquel les demandes CloudFront ont été reçues.

Requêtes

Le nombre de demandes CloudFront reçues de chaque site.

RequestsPct

Le nombre de demandes CloudFront reçues de chaque emplacement en pourcentage du nombre total de demandes CloudFront reçues de tous les sites au cours de la période.

TotalBytes

Le nombre d'octets qui CloudFront ont été diffusés aux spectateurs dans ce pays ou cet État, pour la distribution et la période spécifiées.

Rapport sur les tendances des emplacements

Le rapport inclut les valeurs suivantes :

DistributionID

L'ID de la distribution concernée par le rapport ou `ALL` si le rapport concerne toutes les distributions.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

(Emplacements)

Les colonnes restantes du rapport indiquent les emplacements d'où proviennent les requêtes reçues par CloudFront. Pour plus d'informations sur les valeurs possibles, consultez la description de Location dans Comment les données du rapport de localisation sont-elles liées aux données des journaux CloudFront standard (journaux d'accès).

Comment les données du rapport de localisation sont-elles liées aux données des journaux CloudFront standard (journaux d'accès)

La liste suivante montre comment les données du rapport Locations de la CloudFront console correspondent aux valeurs des journaux CloudFront d'accès. Pour plus d'informations sur les journaux CloudFront d'accès, consultezJournaux d'accès (journaux standard).

Location

Le pays ou U.S... l'état dans lequel se trouve le spectateur. Dans les journaux d'accès, la colonne `c-ip` contient l'adresse IP de l'appareil employé par l'utilisateur. Nous employons des données de géolocalisation pour identifier l'emplacement géographique de l'appareil sur la base de l'adresse IP.

Si vous affichez le rapport Emplacements par pays, la liste des pays est basée sur la norme ISO 3166-2, Codes pour la représentation des noms des pays et de leurs subdivisions – Partie 2 : Codes des subdivisions des pays. La liste des pays inclut les valeurs supplémentaires suivantes :

- Anonymous Proxy (Proxy anonyme) – Requête en provenance d'un proxy anonyme.
- Satellite Provider (Fournisseur satellite) – Requête en provenance d'un fournisseur de services Internet par satellite qui propose ses services à plusieurs pays. Les utilisateurs peuvent se trouver dans des pays avec un risque de fraude élevé.
- Europe (Unknown) (Europe (Inconnu)) – Requête en provenance d'une IP dans un bloc utilisé par plusieurs pays européens. Le pays d'origine de la demande ne peut pas être déterminé. CloudFront utilise Europe (Inconnu) par défaut.
- Asia/Pacific (Inconnu) — La demande provient d'une adresse IP d'un bloc qui est utilisée par plusieurs pays de la Asia/Pacific région. Le pays d'origine de la demande ne peut pas être déterminé. CloudFront utilise Asia/Pacific (Inconnu) par défaut.

Si vous affichez le rapport sur les localisations par U.S État, notez que le rapport peut inclure U.S. territoires et U.S. et des territoires américains.

> **Note**
>
> S'il n'est pas CloudFront possible de déterminer la position d'un utilisateur, celle-ci apparaîtra comme Inconnue dans les rapports des utilisateurs.

Request Count

Le nombre total de demandes provenant du pays ou U.S de l'État dans lequel se trouve le téléspectateur, pour la distribution et la période spécifiées. Cette valeur correspond généralement étroitement au nombre de `GET` demandes provenant d'adresses IP de ce pays ou de cet État dans les journaux CloudFront d'accès.

Requête %

L’une des options suivantes, en fonction de la valeur sélectionnée sous Details (Détails) :

- Countries (Pays) – Les requêtes de ce pays sous la forme d’un pourcentage du nombre total de requêtes.
- U.S. États : demandes provenant de cet État, exprimées en pourcentage du nombre total de demandes provenant des États-Unis.

Si les requêtes proviennent de plus de 50 pays, vous ne pouvez pas calculer Request % (Requête %) sur la base des données de ce tableau, car la colonne Request Count (Nombre de requêtes) n’inclut pas toutes les requêtes pendant la période spécifiée.

Octets

Le nombre d'octets qui CloudFront ont été diffusés aux spectateurs dans ce pays ou cet État, pour la distribution et la période spécifiées. Pour modifier l’affichage des données de cette colonne en Ko, Mo ou Go, choisissez le lien dans l’en-tête de la colonne.

Surveillez CloudFront les métriques avec Amazon CloudWatch

Amazon CloudFront est intégré à Amazon CloudWatch et publie automatiquement les métriques opérationnelles pour les distributions et les fonctions périphériques (Lambda @Edge et CloudFront Functions). Ces métriques peuvent vous aider à résoudre, suivre et déboguer des problèmes. Nombre de ces métriques sont affichées dans un ensemble de graphiques dans la CloudFront console et sont également accessibles à l'aide de l' CloudFront API ou de la CLI. Toutes ces métriques sont disponibles dans la CloudWatch console ou via l' CloudWatch API ou la CLI. CloudFront les métriques ne sont pas prises en compte dans les CloudWatch quotas (anciennement appelés limites) et n'entraînent aucun coût supplémentaire.

Outre les mesures par défaut pour les CloudFront distributions, vous pouvez activer des mesures supplémentaires moyennant des frais supplémentaires. Les mesures supplémentaires s'appliquent aux CloudFront distributions et doivent être activées séparément pour chaque distribution. Pour plus d’informations sur le coût, consultez the section called “Estimez le coût des CloudFront mesures supplémentaires”.

Vous pouvez également définir des alarmes en fonction de ces métriques dans la CloudFront console, ou dans la CloudWatch console, l'API ou la CLI. Par exemple, vous pouvez définir une alarme basée sur la métrique `5xxErrorRate`, qui représente le pourcentage de toutes les

demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse se trouve dans la plage `500` à `599`, incluses. Lorsque le taux d'erreur atteint une certaine valeur pendant un certain laps de temps (par exemple, 5 % des demandes pendant 5 minutes continues), l'alarme est déclenchée. Vous spécifiez la valeur de l'alarme et son unité de temps lorsque vous créez l'alarme.

> **Remarques**
>
> - Lorsque vous créez une CloudWatch alarme dans la CloudFront console, elle en crée une pour vous dans la région USA Est (Virginie du Nord) (`us-east-1`). Si vous créez une alarme à partir de la CloudWatch console, vous devez utiliser la même région. Comme il CloudFront s'agit d'un service mondial, les mesures relatives au service sont envoyées vers l'est des États-Unis (Virginie du Nord).
> - Lors de la création d'alarmes, la CloudWatch tarification standard s'applique.

Rubriques

- Indicateurs CloudFront des fonctions d'affichage et de périphérie
- Création d'alarmes pour les métriques
- Téléchargement des données de métriques au format CSV
- Types de métriques pour CloudFront

Indicateurs CloudFront des fonctions d'affichage et de périphérie

Vous pouvez consulter les statistiques opérationnelles relatives à vos CloudFront distributions et à vos fonctions de périphérie dans la CloudFront console.

Pour afficher CloudFront et contourner les métriques des fonctions dans CloudFront

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Surveillance.
3. Pour afficher des graphiques relatifs à l'activité d'une CloudFront distribution ou d'une fonction de périphérie spécifique, choisissez-en une, puis choisissez Afficher les métriques de distribution ou Afficher les métriques.
4. Vous pouvez personnaliser les graphiques en procédant comme suit :

a. Pour modifier la plage de temps des informations affichées sur les graphiques, choisissez 1h (1 heure), 3h (3 heures) ou une autre plage, ou spécifiez une plage personnalisée.

b. Pour modifier la fréquence de CloudFront mise à jour des informations du graphique, cliquez sur la flèche vers le bas à côté de l'icône d'actualisation, puis choisissez une fréquence de rafraîchissement. Le taux d'actualisation par défaut est d'une minute, mais vous pouvez choisir d'autres options.

5. Pour afficher CloudFront des graphiques dans la CloudWatch console, choisissez Ajouter au tableau de bord. Vous devez utiliser la région USA Est (Virginie du Nord) pour afficher les graphiques dans la CloudWatch console.

Rubriques

- Métriques CloudFront de distribution par défaut
- Activez des métriques CloudFront de distribution supplémentaires
- Métriques de fonction Lambda@Edge par défaut
- Métriques CloudFront des fonctions par défaut

Métriques CloudFront de distribution par défaut

Les métriques par défaut suivantes sont incluses pour toutes les CloudFront distributions, sans frais supplémentaires :

Requêtes

Le nombre total de demandes d'affichage reçues par CloudFront, pour toutes les méthodes HTTP et pour les requêtes HTTP et HTTPS.

Octets téléchargés

Nombre total d'octets téléchargés par les utilisateurs pour les demandes `GET` et `HEAD`.

Octets chargés

Nombre total d'octets vers lesquels les utilisateurs ont transféré CloudFront`OPTIONS`, utilisés `POST` et `PUT` demandés.

Taux d'erreurs 4xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `4xx`.

Taux d’erreurs 5xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `5xx`.

Taux d’erreurs total

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d’état HTTP de la réponse est `4xx` ou `5xx`.

Ces mesures sont affichées sous forme de graphiques pour chaque CloudFront distribution sur la page de surveillance de la CloudFront console. Sur chaque graphique, les totaux sont affichés avec un niveau de précision d’une minute. Outre l’affichage des graphiques, vous pouvez également télécharger des rapports de métriques sous forme de fichiers CSV.

Activez des métriques CloudFront de distribution supplémentaires

En plus des métriques par défaut, vous pouvez activer des métriques supplémentaires pour un coût additionnel. Pour plus d’informations sur le coût, consultez the section called “Estimez le coût des CloudFront mesures supplémentaires”.

Ces métriques supplémentaires doivent être activées séparément pour chaque distribution :

Taux d’accès au cache

Pourcentage de toutes les demandes pouvant être mises en cache pour lesquelles le contenu CloudFront a été diffusé depuis son cache. Les demandes HTTP `POST` et `PUT`, ainsi que les erreurs, ne sont pas considérées comme des requêtes pouvant être mises en cache.

Latence d'origine

Temps total passé entre le moment où une demande est CloudFront reçue et le moment où elle commence à fournir une réponse au réseau (et non à l'utilisateur), pour les demandes traitées depuis l'origine, et non depuis le CloudFront cache. Ceci est également connu sous le nom de latence du premier octet, ou time-to-first-byte.

Taux d'erreur par code d'état

Pourcentage de toutes les requêtes de visionneuse pour lesquelles le code d'état HTTP de la réponse est un code particulier dans la plage `4xx` ou `5xx`. Cette métrique est disponible pour tous les codes d'erreur suivants : `401`, `403`, `404`, `502`, `503` et `504`.

Vous pouvez activer des métriques supplémentaires dans la CloudFront console, avec CloudFormation, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Console

Pour activer des métriques supplémentaires

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Surveillance.
3. Choisissez la distribution pour laquelle vous souhaitez activer des métriques supplémentaires, puis choisissez View distribution metrics (Afficher les métriques de distribution).
4. Choisissez Manage additional metrics (Gérer des indicateurs supplémentaires).
5. Dans la fenêtre Manage additional metrics (Gérer des métriques supplémentaires), activez Enabled (Activé). Lorsque les métriques supplémentaires sont activées, vous pouvez fermer la fenêtre Manage additional metrics (Gérer des métriques supplémentaires).

   Lorsque les métriques supplémentaires sont activées, elles apparaissent dans les graphiques. Sur chaque graphique, les totaux sont affichés avec un niveau de précision d'une minute. Outre l'affichage des graphiques, vous pouvez également télécharger des rapports de métriques sous forme de fichiers CSV.

CloudFormation

Pour activer des métriques supplémentaires avec CloudFormation, utilisez le type de `AWS::CloudFront::MonitoringSubscription` ressource. L'exemple suivant montre la syntaxe du CloudFormation modèle, au format YAML, permettant d'activer des métriques supplémentaires.

```
Type: AWS::CloudFront::MonitoringSubscription
Properties:
  DistributionId: EDFDVBD6EXAMPLE
  MonitoringSubscription:
    RealtimeMetricsSubscriptionConfig:
      RealtimeMetricsSubscriptionStatus: Enabled
```

CLI

Pour gérer des métriques supplémentaires avec le AWS Command Line Interface (AWS CLI), utilisez l'une des commandes suivantes :

Pour activer des métriques supplémentaires pour une distribution

- Utilisez la commande create-monitoring-subscription, comme dans l'exemple suivant. *EDFDVBD6EXAMPLE*Remplacez-le par l'ID de la distribution pour laquelle vous activez des métriques supplémentaires.

```
aws cloudfront create-monitoring-subscription --
distribution-id EDFDVBD6EXAMPLE --monitoring-subscription
 RealtimeMetricsSubscriptionConfig={RealtimeMetricsSubscriptionStatus=Enabled}
```

Pour savoir si des métriques supplémentaires sont activées pour une distribution

- Utilisez la commande get-monitoring-subscription, comme dans l'exemple suivant. *EDFDVBD6EXAMPLE*Remplacez-le par l'ID de la distribution que vous êtes en train de vérifier.

```
aws cloudfront get-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

Pour désactiver des métriques supplémentaires pour une distribution

- Utilisez la commande delete-monitoring-subscription, comme dans l'exemple suivant. *EDFDVBD6EXAMPLE*Remplacez-le par l'ID de la distribution pour laquelle vous désactivez les métriques supplémentaires.

```
aws cloudfront delete-monitoring-subscription --distribution-id EDFDVBD6EXAMPLE
```

API

Pour gérer des métriques supplémentaires avec l' CloudFront API, utilisez l'une des opérations d'API suivantes.

- Pour activer des mesures supplémentaires pour une distribution, utilisez CreateMonitoringSubscription.
- Pour savoir si des métriques supplémentaires sont activées pour une distribution, utilisez GetMonitoringSubscription.
- Pour désactiver des mesures supplémentaires pour une distribution, utilisez DeleteMonitoringSubscription.

Pour plus d'informations sur ces opérations d'API, consultez la documentation de référence de l'API de votre AWS SDK ou d'un autre client d'API.

Estimez le coût des CloudFront mesures supplémentaires

Lorsque vous activez des métriques supplémentaires pour une distribution, CloudFront envoie jusqu'à 8 métriques CloudWatch dans la région USA Est (Virginie du Nord). CloudWatch facture un faible taux fixe pour chaque métrique. Ce tarif n'est facturé qu'une fois par mois, par métrique (jusqu'à 8 métriques par distribution). Il s'agit d'un tarif fixe, de sorte que vos coûts restent les mêmes quel que soit le nombre de demandes ou de réponses que la CloudFront distribution reçoit ou envoie. Pour le tarif par métrique, consultez la page de CloudWatch tarification d'Amazon et le calculateur de CloudWatch prix. Des frais d'API supplémentaires s'appliquent lorsque vous récupérez les métriques avec l' CloudWatch API.

Métriques de fonction Lambda@Edge par défaut

Vous pouvez utiliser CloudWatch des métriques pour surveiller, en temps réel, les problèmes liés à vos fonctions Lambda @Edge. L'utilisation de ces métriques n'implique aucun coût supplémentaire.

Lorsque vous associez une fonction Lambda @Edge à un comportement de cache dans une CloudFront distribution, Lambda commence à envoyer des métriques automatiquement à. CloudWatch Les métriques sont disponibles pour toutes les régions Lambda, mais pour afficher les métriques dans la CloudWatch console ou obtenir les données métriques depuis l' CloudWatch API, vous devez utiliser la région USA Est (Virginie du Nord) (`us-east-1`). Le nom du groupe de métriques est formaté comme suit :`AWS/CloudFront/`*`distribution-ID`*, où *`distribution-ID`* est l'ID de la CloudFront distribution à laquelle la fonction Lambda @Edge est associée. Pour plus d'informations sur CloudWatch les métriques, consultez le guide de CloudWatch l'utilisateur Amazon.

Les métriques par défaut suivantes sont affichées sous forme de graphiques pour chaque fonction Lambda @Edge sur la page Monitoring de la CloudFront console :

- `5xx`Taux d'erreur pour Lambda@Edge
- Erreurs d'exécution Lambda
- Lambda réponses invalides
- Limitations Lambda

Les graphiques incluent les nombres d'appels, d'erreurs, de limitations, etc. Sur chaque graphique, les totaux sont affichés avec un niveau de précision d'une minute, regroupés par région AWS .

Si vous constatez un pic d'erreurs que vous souhaitez examiner, vous pouvez choisir une fonction, puis consulter les fichiers journaux par AWS région, jusqu'à ce que vous déterminiez quelle fonction est à l'origine des problèmes et dans quelle AWS région. Pour de plus amples informations sur le dépannage des erreurs Lambda@Edge, veuillez consulter :

- the section called “Comment déterminer le type d'échec”
- Quatre étapes pour débugger la diffusion de votre contenu sur AWS

Métriques CloudFront des fonctions par défaut

CloudFront Functions envoie des métriques opérationnelles à Amazon CloudWatch afin que vous puissiez surveiller vos fonctions. Ces métriques peut vous aider à résoudre, suivre et déboguer des problèmes. CloudFront Functions publie les métriques suivantes pour CloudWatch :

- Appels (`FunctionInvocations`) – nombre de fois où la fonction a été lancée (appelée) au cours d'une période donnée.
- Erreurs de validation (`FunctionValidationErrors`) – nombre d'erreurs de validation générées par la fonction au cours d'une période donnée. Des erreurs de validation se produisent lorsque la fonction s'exécute correctement, mais renvoie des données non valides (un objet d'événement non valide).
- Erreurs d'exécution (`FunctionExecutionErrors`) – nombre d'erreurs d'exécution survenues au cours d'une période donnée. Des erreurs d'exécution se produisent lorsque la fonction échoue.
- Utilisation du calcul (`FunctionComputeUtilization`) – durée d'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une valeur de 35 signifie que la durée d'exécution de la fonction représente 35 % du temps maximum autorisé. Cette métrique est un nombre compris entre 0 et 100.

Si cette valeur atteint 100 ou s'en approche, cela signifie que la fonction a utilisé ou est sur le point d'utiliser le temps d'exécution autorisé, et les demandes suivantes pourraient être limitées. Si votre fonction fonctionne avec un taux d'utilisation de 80 % ou plus, nous vous recommandons d'examiner votre fonction afin d'en réduire le temps d'exécution et d'améliorer son utilisation. Par exemple, vous pouvez choisir de ne consigner que les erreurs, de simplifier des expressions regex complexes ou de supprimer l'analyse inutile d'objets JSON complexes.

- Limitations(`FunctionThrottles`) – nombre de fois où la fonction a été limitée au cours d'une période donnée. Les fonctions peuvent être limitées pour les raisons suivantes :
  - La fonction dépasse continuellement la durée maximale autorisée pour l'exécution.
  - La fonction entraîne des erreurs de compilation.
  - Le nombre de demandes par seconde est exceptionnellement élevé.

CloudFront KeyValueStore envoie également les métriques opérationnelles suivantes à Amazon CloudWatch :

- Demandes de lecture (`KvsReadRequests`) : nombre de fois où la fonction a réussi à lire dans le magasin de clés-valeurs au cours d'une période donnée.
- Erreurs de lecture (`KvsReadErrors`) : nombre de fois où la fonction n'a pas réussi à lire dans le magasin de clés-valeurs durant une période donnée.

Toutes ces métriques sont publiées CloudWatch dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`), dans l'espace de CloudFront noms. Vous pouvez également consulter ces statistiques dans la CloudWatch console. Dans la CloudWatch console, vous pouvez consulter les métriques par fonction ou par fonction par distribution.

Vous pouvez également l'utiliser CloudWatch pour définir des alarmes en fonction de ces mesures. Par exemple, vous pouvez définir une alarme basée sur la métrique du temps d'exécution (`FunctionComputeUtilization`), qui représente le pourcentage du temps disponible que votre fonction a pris pour s'exécuter. Lorsque le temps d'exécution atteint une certaine valeur pendant une durée déterminée. Par exemple, si vous choisissez supérieur à 70 % du temps disponible pendant 15 minutes consécutives, l'alarme se déclenche. Vous spécifiez la valeur de l'alarme et son unité de temps lorsque vous créez l'alarme.

> **Note**
>
> CloudFront Functions envoie des métriques CloudWatch uniquement pour les fonctions de la `LIVE` phase qui s'exécutent en réponse aux demandes et réponses de production. Lorsque vous testez une fonction, CloudFront elle n'envoie aucune métrique à CloudWatch. Le résultat du test contient des informations sur les erreurs, l'utilisation du calcul et les journaux de fonctionnement (`console.log()`instructions), mais ces informations ne sont pas envoyées à CloudWatch.

Pour plus d'informations sur la façon d'obtenir ces métriques avec l' CloudWatch API, consultezthe section called “CloudFront métriques”.

Création d'alarmes pour les métriques

Dans la CloudFront console, vous pouvez définir des alarmes pour qu'elles vous avertissent par Amazon Simple Notification Service (Amazon SNS) en fonction de mesures spécifiques. CloudFront

Pour créer des alarmes pour les métriques

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, cliquez sur Alarms (Alarmes).
3. Sélectionnez Créer une alarme.
4. Pour Détails, spécifiez les paramètres suivants :
   a. Nom de l’alarme : un nom pour l’alarme.
   b. Distribution : CloudFront distribution pour laquelle vous créez l'alarme.
5. Pour Condition, spécifiez ce qui suit :
   a. Métrique : la métrique pour laquelle vous créez l’alarme.
   b. « SI » <condition>: seuil à partir duquel une alarme CloudWatch doit être déclenchée et une notification doit être envoyée à la rubrique Amazon SNS. Par exemple, pour recevoir une notification lorsque le taux d'erreurs `5xx` dépasse 1 %, spécifiez ce qui suit :

      Taux d’erreurs 5xx > 1

c. « PENDANT » périodes consécutives : la durée pendant laquelle la condition doit être remplie avant de déclencher une alarme. Lorsque vous choisissez une valeur, essayez de trouver l'équilibre approprié entre une valeur qui ne déclenche par une alarme pour des problèmes temporaires, mais qui en déclenche une pour des problèmes durables ou réels.

d. (Facultatif) Notification : la rubrique Amazon SNS à laquelle envoyer une notification si cette métrique déclenche une alarme.

6. Sélectionnez Créer une alerte.

> **Remarques**
>
> - Lorsque vous entrez les valeurs de la condition, utilisez des nombres entiers sans ponctuation. Par exemple, pour spécifier mille, entrez **`1000`**.
> - Pour `4xx`, `5xx` et les taux de nombre total d'erreurs, vous spécifiez un pourcentage.
> - Pour les requêtes, les octets téléchargés et les octets chargés, vous spécifiez des unités. Par exemple, 1073742000 octets.

Pour plus d'informations sur la création de rubriques Amazon SNS, consultez Création d'une rubrique Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

Téléchargement des données de métriques au format CSV

Vous pouvez télécharger les données CloudWatch métriques d'une CloudFront distribution au format CSV.

Pour télécharger des données de métriques au format CSV

1. Connectez-vous à la CloudFront console Console de gestion AWS et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation, choisissez Surveillance.
3. Choisissez la distribution, puis sélectionnez Afficher les métriques de distribution.
4. Choisissez Télécharger le rapport CSV, puis sélectionnez la période souhaitée (par exemple, Pour le dernier jour (période d'une heure).
5. Une fois le fichier téléchargé, ouvrez-le pour afficher les informations suivantes.

Rubriques

- Informations sur le rapport
- Données du rapport Metrics

Informations sur le rapport

Les toutes premières lignes du rapport incluent les informations suivantes :

Version

La version CloudFront de rapport.

Rapport

Nom du rapport.

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

StartDateUTC

Début de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

EndDateUTC

Fin de la plage de dates pour laquelle vous avez exécuté le rapport, en heure UTC.

GeneratedTimeUTC

Date et heure auxquelles vous avez exécuté le rapport, en heure UTC.

Granularité

Durée de chaque ligne du rapport, par exemple, `ONE_MINUTE`.

Données du rapport Metrics

Le rapport inclut les valeurs suivantes :

DistributionID

ID de la distribution pour laquelle vous avez exécuté le rapport.

FriendlyName

Nom de domaine alternatif (CNAME) de la distribution, le cas échéant. Si une distribution ne comporte pas de noms de domaines alternatifs, la liste inclut un nom de domaine d'origine pour la distribution.

TimeBucket

L'heure du jour correspondant aux données, en heure UTC (temps universel coordonné).

Requêtes

Nombre total de demandes pour tous les codes d'état HTTP (par exemple, `200`, `404`, etc.) et toutes les méthodes (par exemple, `GET`, `HEAD`, `POST`) pendant la période.

BytesDownloaded

Nombre d'octets que les utilisateurs ont téléchargé pour la distribution spécifiée pendant la période.

BytesUploaded

Nombre d'octets que les utilisateurs ont chargé pour la distribution spécifiée pendant la période.

TotalErrorRatePct

Pourcentage des requêtes pour lesquelles le code d'état HTTP était une erreur `4xx` ou `5xx` pour la distribution spécifiée pendant la période.

4 xxErrorRate pct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `4xx` pour la distribution spécifiée pendant la période.

5 xxErrorRate pct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `5xx` pour la distribution spécifiée pendant la période.

Si vous avez activé des métriques supplémentaires pour votre distribution, le rapport inclut également les valeurs supplémentaires suivantes :

401 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `401` pour la distribution spécifiée pendant la période.

403 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `403` pour la distribution spécifiée pendant la période.

404 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `404` pour la distribution spécifiée pendant la période.

502 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `502` pour la distribution spécifiée pendant la période.

503 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `503` pour la distribution spécifiée pendant la période.

504 ErrorRatePct

Pourcentage de requêtes pour lesquelles le code d'état HTTP était une erreur `504` pour la distribution spécifiée pendant la période.

OriginLatency

Temps total passé, en millisecondes, entre le moment où une demande CloudFront a été reçue et le moment où elle a commencé à fournir une réponse au réseau (et non au téléspectateur), pour les demandes traitées depuis l'origine, et non depuis le cache. CloudFront Ceci est également connu sous le nom de latence du premier octet, ou time-to-first-byte.

CacheHitRate

Pourcentage de toutes les demandes pouvant être mises en cache pour lesquelles le contenu CloudFront a été diffusé depuis son cache. Les demandes HTTP `POST` et `PUT`, ainsi que les erreurs, ne sont pas considérées comme des requêtes pouvant être mises en cache.

Types de métriques pour CloudFront

Vous pouvez utiliser l' CloudWatch API ou AWS Command Line Interface (AWS CLI) pour obtenir les CloudFront métriques dans les programmes ou les applications que vous créez. Vous pouvez

utiliser les données brutes pour créer vos propres tableaux de bord personnalisés, vos propres outils d'alarme, etc.

Pour plus d'informations, consultez get-metric-datala référence des AWS CLI commandes ou le fonctionnement de l'GetMetricDataAPI dans la référence des CloudWatch API Amazon.

Rubriques

- Valeurs pour tous les CloudFront indicateurs
- Valeurs pour les métriques CloudFront de distribution
- Valeurs pour les métriques des CloudFront fonctions

> **Note**
>
> Pour obtenir les CloudFront métriques à partir de l' CloudWatch API, vous devez utiliser la région USA Est (Virginie du Nord) (`us-east-1`). Vous devez également connaître certaines valeurs et types pour chaque métrique.

Valeurs pour tous les CloudFront indicateurs

Les valeurs suivantes s'appliquent à toutes les CloudFront mesures :

`Namespace`

La valeur pour `Namespace` est toujours `AWS/CloudFront`.

Dimensions

Chaque CloudFront métrique possède les dimensions suivantes :

`DistributionId`

L'ID de la CloudFront distribution pour laquelle vous souhaitez obtenir des métriques.

`FunctionName`

Nom de la fonction (dans CloudFront Fonctions) pour laquelle vous souhaitez obtenir des métriques.

Cette dimension s'applique uniquement aux fonctions.

`Region`

La valeur pour « `Region` c'est toujours `Global` parce que CloudFront c'est un service mondial ».

Valeurs pour les métriques CloudFront de distribution

Utilisez les informations de la liste suivante pour obtenir des informations sur des métriques de CloudFront distribution spécifiques à partir de l' CloudWatch API. Certaines de ces métriques sont disponibles uniquement lorsque vous avez activé les métriques supplémentaires pour la distribution.

> **Note**
>
> Une seule statistique, `Average` ou `Sum`, est applicable à chaque métrique. La liste suivante indique quelle statistique est applicable à cette métrique.

Taux d’erreurs 4xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d’état HTTP de la réponse est `4xx`.

- Nom de métrique : `4xxErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 401

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `401`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `401ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 403

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `403`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `403ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 404

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `404`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `404ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 5xx

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d’état HTTP de la réponse est `5xx`.

- Nom de métrique : `5xxErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 502

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `502`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `502ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 503

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `503`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `503ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Taux d’erreurs 504

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d'état HTTP de la réponse est `504`. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `504ErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Octets téléchargés

Nombre total d’octets téléchargés par les utilisateurs pour les demandes `GET` et `HEAD`.

- Nom de métrique : `BytesDownloaded`
- Statistique valide : `Sum`
- Unité : `None`

Octets chargés

Nombre total d'octets vers lesquels les utilisateurs ont transféré CloudFront`OPTIONS`, utilisés `POST` et `PUT` demandés.

- Nom de métrique : `BytesUploaded`
- Statistique valide : `Sum`
- Unité : `None`

Taux d’accès au cache

Pourcentage de toutes les demandes pouvant être mises en cache pour lesquelles le contenu CloudFront a été diffusé depuis son cache. Les demandes HTTP `POST` et `PUT`, ainsi que les erreurs, ne sont pas considérées comme des requêtes pouvant être mises en cache. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `CacheHitRate`
- Statistique valide : `Average`
- Unité : `Percent`

Latence d'origine

Temps total passé, en millisecondes, entre le moment où une demande est CloudFront reçue et le moment où elle commence à fournir une réponse au réseau (et non à l'utilisateur), pour les

demandes traitées depuis l'origine, et non depuis le cache. CloudFront Ceci est également connu sous le nom de latence du premier octet, ou time-to-first-byte. Pour obtenir cette métrique, vous devez d'abord activer les métriques supplémentaires.

- Nom de métrique : `OriginLatency`
- Statistique valide : `Percentile`
- Unité : `Milliseconds`

> **Note**
>
> Pour obtenir une `Percentile` statistique à partir de l' CloudWatch API, utilisez le `ExtendedStatistics` paramètre, not`Statistics`. Pour plus d'informations, consultez GetMetricStatisticsle manuel Amazon CloudWatch API Reference ou la documentation de référence du AWS SDKs.

Requêtes

Le nombre total de demandes d'affichage reçues par CloudFront, pour toutes les méthodes HTTP et pour les requêtes HTTP et HTTPS.

- Nom de métrique : `Requests`
- Statistique valide : `Sum`
- Unité : `None`

Taux d’erreurs total

Pourcentage de toutes les demandes de visionneuse pour lesquelles le code d’état HTTP de la réponse est `4xx` ou `5xx`.

- Nom de métrique : `TotalErrorRate`
- Statistique valide : `Average`
- Unité : `Percent`

Valeurs pour les métriques des CloudFront fonctions

Utilisez les informations de la liste suivante pour obtenir des informations sur des métriques de CloudFront fonction spécifiques à partir de l' CloudWatch API.

> **Note**
>
> Une seule statistique, `Average` ou `Sum`, est applicable à chaque métrique. La liste suivante indique quelle statistique est applicable à cette métrique.

Appels

Nombre de fois où la fonction a été démarrée (appelée) au cours d'une période donnée.

- Nom de métrique : `FunctionInvocations`
- Statistique valide : `Sum`
- Unité : `None`

Erreurs de validation

Nombre d'erreurs de validation générées par la fonction au cours d'une période donnée. Des erreurs de validation se produisent lorsque la fonction s'exécute correctement, mais renvoie des données non valides (un objet d'événement non valide).

- Nom de métrique : `FunctionValidationErrors`
- Statistique valide : `Sum`
- Unité : `None`

Erreurs d'exécution

Nombre d'erreurs d'exécution générées au cours d'une période donnée. Des erreurs d'exécution se produisent lorsque la fonction échoue.

- Nom de métrique : `FunctionExecutionErrors`
- Statistique valide : `Sum`
- Unité : `None`

Utilisation du calcul

Durée nécessaire (0-100) pour l'exécution de la fonction en pourcentage de la durée maximale autorisée. Par exemple, une valeur de 35 signifie que la durée d’exécution de la fonction représente 35 % du temps maximum autorisé.

- Nom de métrique : `FunctionComputeUtilization`
- Statistique valide : `Average`
- Unité : `Percent`

Throttles

Nombre de fois où la fonction a été limitée au cours d'une période donnée.

- Nom de métrique : `FunctionThrottles`
- Statistique valide : `Sum`
- Unité : `None`

CloudFront et journalisation des fonctions Edge

Amazon CloudFront propose différents types de journalisation. Vous pouvez enregistrer les demandes des utilisateurs qui arrivent à vos CloudFront distributions, ou vous pouvez enregistrer l'activité du CloudFront service (activité de l'API) dans votre AWS compte. Vous pouvez également obtenir des journaux à partir de vos CloudFront fonctions Functions et Lambda @Edge.

Demandes d'enregistrement

CloudFront fournit les méthodes suivantes pour enregistrer les demandes envoyées à vos distributions.

Journaux d'accès (journaux standard)

CloudFrontles journaux d'accès fournissent des informations détaillées sur chaque demande adressée à une distribution. Vous pouvez utiliser les journaux pour des scénarios, tels que des audits de sécurité et d’accès.

CloudFrontles journaux d'accès sont envoyés à la destination de livraison que vous spécifiez.

Utilisez les journaux d'accès lorsque vous avez besoin de :

- Analyse historique et rapports
- Audits de sécurité et exigences de conformité
- Conservation rentable des journaux à long terme

Pour de plus amples informations, veuillez consulter Journaux d'accès (journaux standard).

Journaux d’accès en temps réel

CloudFrontles journaux d'accès en temps réel sont fournis quelques secondes après réception des demandes et fournissent des informations sur les demandes adressées à une distribution

en temps réel. Vous pouvez choisir le taux d'échantillonnage pour vos journaux d'accès en temps réel, c'est-à-dire le pourcentage de demandes pour lesquelles vous souhaitez recevoir des enregistrements de journaux d'accès en temps réel. Vous pouvez également choisir les champs que vous souhaitez recevoir dans les enregistrements de journaux. Les journaux d'accès en temps réel sont idéaux pour surveiller en direct les performances de diffusion de contenu.

CloudFront les journaux d'accès en temps réel sont transmis au flux de données de votre choix dans Amazon Kinesis Data Streams. CloudFront des frais pour les journaux d'accès en temps réel, en plus des frais que vous devez payer pour utiliser Kinesis Data Streams.

Utilisez des journaux d'accès en temps réel lorsque vous avez besoin de :

- Surveillance et alertes en temps réel
- Tableaux de bord en direct et informations opérationnelles

Pour de plus amples informations, veuillez consulter Utiliser des journaux d'accès en temps réel.

Journaux de connexion.

Les journaux de connexion fournissent des informations détaillées sur la connexion entre le serveur et le client pour les distributions compatibles mTLS. Les journaux de connexion fournissent une visibilité sur les informations relatives aux certificats clients, les raisons des échecs d'authentification MTL et indiquent si une connexion a été autorisée ou refusée.

Tout comme les journaux d'accès (journaux standard), les journaux de connexion sont envoyés à la destination de livraison que vous spécifiez.

> **Note**
>
> Pour activer les journaux de connexion, vous devez d'abord activer les MTL pour votre distribution.

Utilisez les journaux de connexion lorsque vous avez besoin de :

- Raisons de la réussite ou de l'échec des connexions lors de la prise de contact TLS
- Visibilité des informations relatives aux certificats clients

Pour de plus amples informations, veuillez consulter Observabilité à l'aide des journaux de connexion.

Journalisation des fonctions de périphérie

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir les journaux de vos fonctions périphériques, à la fois Lambda @Edge et CloudFront Functions. Vous pouvez accéder aux journaux à l'aide de la CloudWatch console ou de l'API CloudWatch Logs. Pour de plus amples informations, veuillez consulter the section called “Journaux des fonctions de périphérie”.

Activité de service de journalisation

Vous pouvez l'utiliser AWS CloudTrail pour enregistrer l'activité du CloudFront service (activité de l'API) dans votre AWS compte. CloudTrail fournit un enregistrement des actions d'API effectuées par un utilisateur, un rôle ou un AWS service dans CloudFront. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande d'API qui a été faite CloudFront, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour de plus amples informations, veuillez consulter Journalisation des appels CloudFront d'API Amazon à l'aide AWS CloudTrail.

Pour plus d’informations sur la journalisation, consultez les rubriques suivantes :

Rubriques

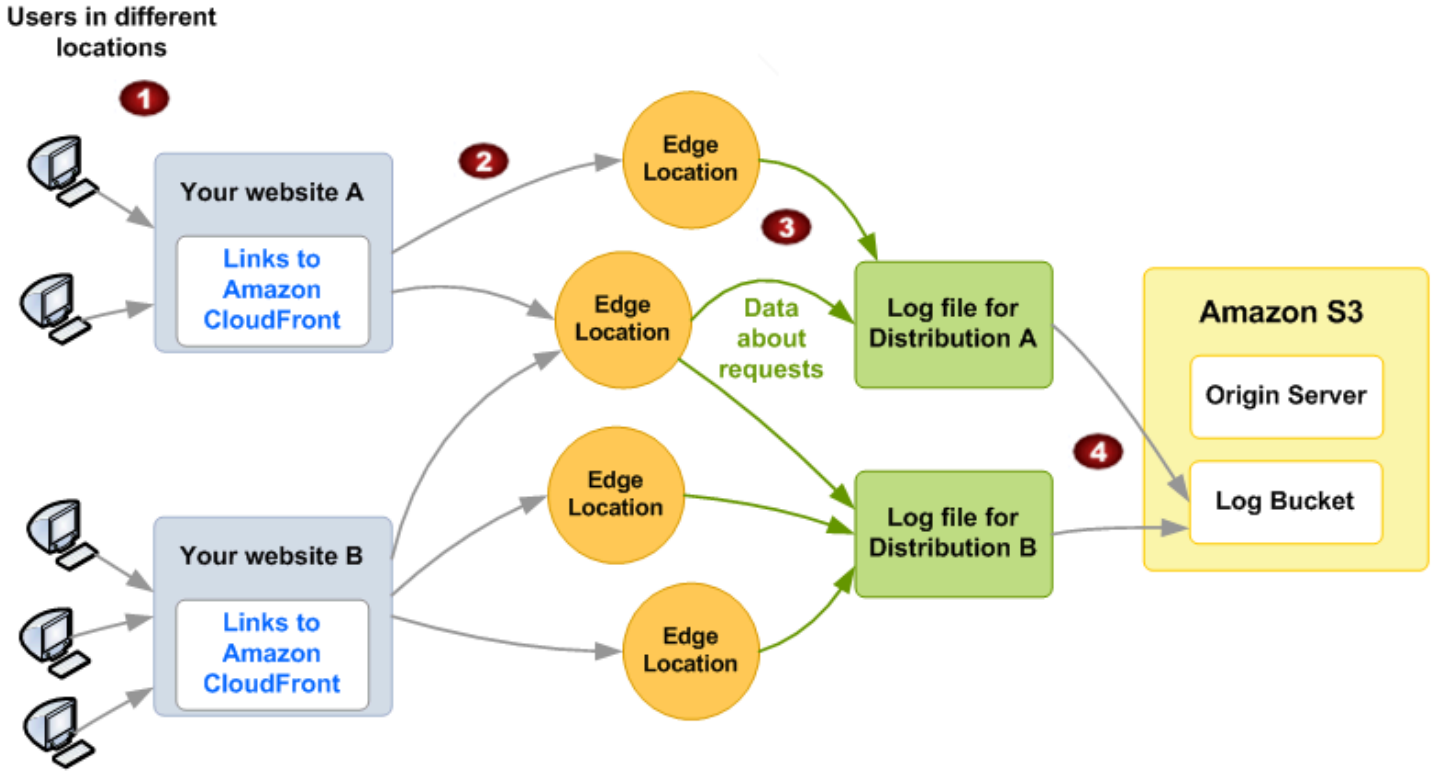
- Journaux d'accès (journaux standard)
- Utiliser des journaux d'accès en temps réel
- Journaux des fonctions de périphérie
- Journalisation des appels CloudFront d'API Amazon à l'aide AWS CloudTrail

Journaux d'accès (journaux standard)

Vous pouvez configurer CloudFront pour créer des fichiers journaux contenant des informations détaillées sur chaque demande d'utilisateur (utilisateur) CloudFront reçue. Ces journaux sont appelés journaux d'accès, également appelés journaux standard.

Chaque journal contient des informations comme l’heure à laquelle la demande a été reçue, l’heure du traitement, les chemins de demande et les réponses du serveur. Vous pouvez utiliser ces journaux d’accès pour analyser les modèles de trafic et résoudre des problèmes.

Le schéma suivant montre comment CloudFront enregistre les informations relatives aux demandes concernant vos objets. Dans cet exemple, les distributions sont configurées pour envoyer les journaux d'accès vers un compartiment Amazon S3.



1. Dans cet exemple, vous avez deux sites Web, A et B, et deux CloudFront distributions correspondantes. Les utilisateurs demandent vos objets à l'aide des URL associées à vos distributions.
2. CloudFront achemine chaque demande vers l'emplacement périphérique approprié.
3. CloudFront écrit les données relatives à chaque demande dans un fichier journal spécifique à cette distribution. Dans cet exemple, les informations sur les demandes associées à Distribution A vont dans un fichier journal réservé à Distribution A et celles sur les demandes associées à Distribution B dans un fichier journal réservé à Distribution B.
4. CloudFront enregistre régulièrement le fichier journal d'une distribution dans le compartiment Amazon S3 que vous avez spécifié lorsque vous avez activé la journalisation. CloudFront commence ensuite à enregistrer les informations relatives aux demandes suivantes dans un nouveau fichier journal pour la distribution.

   Si aucun utilisateur n'accède à votre contenu pendant une heure donnée, vous ne recevez aucun fichier journal pour cette heure.

> **Note**
>
> Nous vous recommandons d'utiliser les journaux pour comprendre la nature des demandes concernant votre contenu, et non pour comptabiliser toutes les demandes. CloudFront fournit des journaux d'accès dans les meilleurs délais. L'entrée de journal pour une demande particulière peut être envoyée longtemps après le traitement de la demande. Dans de rares cas, une entrée de journal peut ne pas être transmise du tout. Quand une entrée du journal est omise des journaux d'accès, le nombre d'entrées des journaux d'accès ne correspond pas à l'utilisation qui apparaît dans les rapports d'utilisation et de facturation AWS .

CloudFront prend en charge deux versions de la journalisation standard. La journalisation standard (héritée) prend uniquement en charge l'envoi des journaux d'accès vers Amazon S3. La journalisation standard (v2) prend en charge des destinations de livraison supplémentaires. Vous pouvez configurer les deux options de journalisation, ou seulement l'une d'entre elles, pour votre distribution. Pour plus d'informations, consultez les rubriques suivantes :

Rubriques

- Configuration de la journalisation standard (v2)
- Configurer la journalisation standard (héritée)
- Référence de la journalisation standard

> **Tip**
>
> CloudFront propose également des journaux d'accès en temps réel, qui vous fournissent des informations sur les demandes adressées à une distribution en temps réel (les journaux sont fournis quelques secondes après réception des demandes). Vous pouvez utiliser les journaux d'accès en temps réel pour surveiller, analyser et prendre des mesures en fonction des performances de diffusion de contenu. Pour plus d'informations, consultez Utiliser des journaux d'accès en temps réel.

Configuration de la journalisation standard (v2)

Vous pouvez activer les journaux d'accès (journaux standard) lorsque vous créez ou mettez à jour une distribution. La journalisation standard (v2) comprend les fonctionnalités suivantes :

- Envoyez les journaux d'accès à Amazon CloudWatch Logs, Amazon Data Firehose et Amazon Simple Storage Service (Amazon S3).
- La sélection des champs de journal souhaités. Vous pouvez également sélectionner un sous-ensemble de champs du journal d'accès en temps réel.
- La sélection d'autres formats de fichiers journaux de sortie.

Si vous utilisez Amazon S3, vous disposez des fonctionnalités optionnelles suivantes :

- Envoyez des journaux pour vous inscrire. Régions AWS
- Organisation des journaux à l'aide du partitionnement.
- Activez les noms de Hive-compatible fichiers.

Pour de plus amples informations, veuillez consulter Envoi de journaux vers Amazon S3.

Pour commencer avec la journalisation standard, procédez comme suit :

1. Configurez les autorisations requises pour la personne spécifiée Service AWS qui recevra vos journaux.
2. Configurez la journalisation standard à partir de la CloudFront console ou de l' CloudWatch API.
3. Affichez vos journaux d'accès.

> **Note**
>
> - L'activation de la journalisation standard (v2) n'a aucun impact sur la journalisation standard (héritée). Vous pouvez continuer à utiliser la journalisation standard (héritée) pour votre distribution, en plus de la journalisation standard (v2). Pour plus d'informations, consultez Configurer la journalisation standard (héritée).
> - Si vous utilisez déjà la journalisation standard (héritée) et que vous souhaitez activer la journalisation standard (v2) sur Amazon S3, nous vous conseillons d'indiquer un compartiment Amazon S3 différent ou d'utiliser un chemin distinct dans le même compartiment (par exemple, un préfixe de journal ou un partitionnement). Vous pouvez ainsi facilement identifier les fichiers journaux associés à chaque distribution, tout en évitant qu'ils ne se remplacent mutuellement.

Permissions

CloudFront utilise des CloudWatch journaux vendus pour fournir des journaux d'accès. Pour ce faire, vous devez disposer des autorisations relatives à ce qui Service AWS est spécifié afin de pouvoir activer la livraison des journaux.

Pour connaître les autorisations requises pour chaque destination de journalisation, choisissez l'une des rubriques suivantes dans le guide de l'utilisateur Amazon CloudWatch Logs.

- CloudWatch Journaux
- Firehose
- Amazon S3

Une fois les autorisations configurées pour votre destination de journalisation, vous pouvez activer la journalisation standard sur votre distribution.

> **Note**
>
> CloudFront prend en charge l'envoi de journaux d'accès à différents Comptes AWS (comptes croisés). Pour activer la livraison entre comptes, les deux comptes (le vôtre et celui du destinataire) doivent disposer des autorisations requises. Pour plus d'informations, consultez la Activation de la journalisation standard pour la livraison entre comptes section ou l'exemple Cross-account de livraison dans le guide de l'utilisateur Amazon CloudWatch Logs.

Activation de la journalisation standard

Pour activer la journalisation standard, vous pouvez utiliser la CloudFront console ou l' CloudWatch API.

Table des matières

- Activer la journalisation standard (CloudFront console)
- Activer la journalisation standard (CloudWatch API)

Activer la journalisation standard (CloudFront console)

Pour activer la journalisation standard pour une CloudFront distribution (console)

1. Utilisez la CloudFront console pour mettre à jour une distribution existante.
2. Sélectionnez l'onglet Logging (Journalisation).
3. Choisissez Ajouter, puis sélectionnez le service qui recevra vos journaux :
   - CloudWatch Journaux
   - Firehose
   - Amazon S3
4. Pour la Destination, sélectionnez la ressource correspondant à votre service. Si vous n'avez pas encore créé votre ressource, vous pouvez sélectionner Créer ou consulter la documentation ci-dessous.
   - Pour CloudWatch Logs, entrez le nom du groupe de logs.
   - Pour Firehose, saisissez le Flux de diffusion Firehose.
   - Pour Amazon S3, saisissez le Nom du compartiment.

   > **Tip**
   >
   > Pour ajouter un préfixe, saisissez-le après le nom du compartiment, par exemple `amzn-s3-demo-bucket.s3.amazonaws.com/MyLogPrefix`. Si vous ne spécifiez pas de préfixe, il en CloudFront ajoutera automatiquement un pour vous. Pour de plus amples informations, veuillez consulter Envoi de journaux vers Amazon S3.
5. Pour Paramètres supplémentaires – facultatif, vous pouvez définir les options suivantes :
   a. Pour la Sélection des champs, sélectionnez les noms de champs de journaux que vous souhaitez envoyer vers votre destination. Vous pouvez sélectionner les champs du journal d'accès et un sous-ensemble de champs du journal d'accès en temps réel.
   b. (Amazon S3 uniquement) Pour le Partitionnement, indiquez le chemin permettant de partitionner les données de votre fichier journal.
   c. (Amazon S3 uniquement) Pour Hive-compatible le format de fichier, vous pouvez cocher la case pour utiliser les chemins Hive-compatible S3. Cela permet de simplifier le chargement de nouvelles données dans vos Hive-compatible outils.
   d. Pour Format de sortie, indiquez le format que vous souhaitez utiliser.

> **Note**
>
> Si vous choisissez Parquet, cette option entraîne des CloudWatch frais pour la conversion de vos journaux d'accès vers Apache Parquet. Pour plus d'informations, consultez la section Vended Logs pour CloudWatch connaître les tarifs.

e. Pour Délimiteur de champ, indiquez comment séparer les champs du journal.

6. Terminez les étapes pour mettre à jour ou créer votre distribution.
7. Pour ajouter une autre destination, répétez les étapes 3 à 6.
8. Sur la page Journaux, vérifiez que l'état des journaux standard est défini sur Activé à côté de la distribution.
9. (Facultatif) Pour activer l'enregistrement des cookies, choisissez Gérer, Paramètres et activez Journalisation des cookies, puis sélectionnez Enregistrer les modifications.

> **Tip**
>
> La journalisation des cookies est un paramètre global qui s'applique à l'ensemble de la journalisation standard de votre distribution. Vous ne pouvez pas remplacer ce paramètre pour des destinations de livraison distinctes.

Pour plus d'informations sur la livraison de la journalisation standard et les champs de journal, consultez la Référence de la journalisation standard.

Activer la journalisation standard (CloudWatch API)

Vous pouvez également utiliser l' CloudWatch API pour activer la journalisation standard pour vos distributions.

> **Remarques**
>
> - Lorsque vous appelez l' CloudWatch API pour activer la journalisation standard, vous devez spécifier la région des États-Unis Est (Virginie du Nord`us-east-1`) (), même si vous souhaitez activer la livraison entre régions vers une autre destination. Par exemple, si vous souhaitez envoyer vos journaux d'accès à un compartiment S3 dans la région Europe (Irlande) `eu-west-1` (), utilisez CloudWatch l'API de `us-east-1` la région.

- Une option supplémentaire permet d'inclure les cookies dans la journalisation standard. Dans l' CloudFront API, il s'agit du `IncludeCookies` paramètre. Si vous configurez la journalisation des accès à l'aide de l' CloudWatch API et que vous spécifiez que vous souhaitez inclure des cookies, vous devez utiliser la CloudFront console ou l' CloudFront API pour mettre à jour votre distribution afin d'inclure les cookies. Dans le cas contraire, CloudFront vous ne pourrez pas envoyer de cookies à la destination de votre journal. Pour de plus amples informations, veuillez consulter Journalisation des cookies.

Pour activer la journalisation standard pour une distribution (CloudWatch API)

1. Après avoir créé une distribution, récupérez l'Amazon Resource Name (ARN).

   Vous pouvez trouver l'ARN sur la page de distribution de la CloudFront console ou vous pouvez utiliser l'opération GetDistributionAPI. L'ARN d'une distribution suit le format suivant : `arn:aws:cloudfront::123456789012:distribution/d111111abcdef8`
2. Utilisez ensuite l'opération CloudWatch PutDeliverySourceAPI pour créer une source de diffusion pour la distribution.

   a. Entrez un nom pour la source de livraison.

   b. Indiquez le `resourceArn` de la distribution.

   c. Pour `logType`, indiquez `ACCESS_LOGS` comme type de journaux à collecter.

   d. Example Exemple AWS CLI commande put-delivery-source

      Voici un exemple de configuration d'une source de livraison pour une distribution.

```
aws logs put-delivery-source --name S3-delivery --resource-arn
 arn:aws:cloudfront::123456789012:distribution/d111111abcdef8 --log-type
 ACCESS_LOGS
```

      Sortie

```
{
 "deliverySource": {
 "name": "S3-delivery",
 "arn": "arn:aws:logs:us-east-1:123456789012:delivery-source:S3-delivery",
 "resourceArns": [
 "arn:aws:cloudfront::123456789012:distribution/d111111abcdef8"
```

```
 ],
 "service": "cloudfront",
 "logType": "ACCESS_LOGS"
 }
}
```

3. Utilisez l'opération PutDeliveryDestinationAPI pour configurer l'emplacement de stockage de vos journaux.

   a. Renseignez l'ARN de la destination dans le paramètre `destinationResourceArn`. Il peut s'agir d'un groupe de CloudWatch journaux, d'un flux de diffusion Firehose ou d'un compartiment Amazon S3.

   b. Indiquez le format de sortie de vos journaux dans le paramètre `outputFormat`.

   c. Example Exemple AWS CLI commande put-delivery-destination

      Voici un exemple de configuration d'une destination de livraison vers un compartiment Amazon S3.

```
aws logs put-delivery-destination --name S3-destination --delivery-destination-
configuration destinationResourceArn=arn:aws:s3:::amzn-s3-demo-bucket
```

      Sortie

```
{
    "name": "S3-destination",
    "arn": "arn:aws:logs:us-east-1:123456789012:delivery-destination:S3-
destination",
    "deliveryDestinationType": "S3",
    "deliveryDestinationConfiguration": {
        "destinationResourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
}
```

> **Note**
>
> Si vous distribuez des journaux entre comptes, vous devez utiliser l'opération PutDeliveryDestinationPolicyAPI pour attribuer une politique Gestion des identités et des

accès AWS (IAM) au compte de destination. La politique IAM autorise la livraison d'un compte à un autre.

4. Utilisez l'opération CreateDeliveryAPI pour lier la source de livraison à la destination que vous avez créée lors des étapes précédentes. Cette opération d'API associe la source de livraison à la destination finale.

   a. Indiquez le nom de la source dans le paramètre `deliverySourceName`.
   b. Indiquez l'ARN correspondant à la destination de livraison dans le paramètre `deliveryDestinationArn`.
   c. Indiquez la chaîne qui séparera les champs du journal dans le paramètre `fieldDelimiter`.
   d. Indiquez les champs de journal souhaités dans le paramètre `recordFields`.
   e. Si vous utilisez S3, indiquez s'il faut activer `enableHiveCompatiblePath` et `suffixPath`.

   Example Exemple AWS CLI commande create-delivery

   Voici un exemple de création d'une livraison.

```
aws logs create-delivery --delivery-source-name cf-delivery --delivery-destination-
arn arn:aws:logs:us-east-1:123456789012:delivery-destination:S3-destination
```

   Sortie

```
{
    "id": "abcNegnBoTR123",
    "arn": "arn:aws:logs:us-east-1:123456789012:delivery:abcNegnBoTR123",
    "deliverySourceName": "cf-delivery",
    "deliveryDestinationArn": "arn:aws:logs:us-east-1:123456789012:delivery-
destination:S3-destination",
    "deliveryDestinationType": "S3",
    "recordFields": [
        "date",
        "time",
        "x-edge-location",
        "sc-bytes",
        "c-ip",
        "cs-method",
```

```
        "cs(Host)",
        "cs-uri-stem",
        "sc-status",
        "cs(Referer)",
        "cs(User-Agent)",
        "cs-uri-query",
        "cs(Cookie)",
        "x-edge-result-type",
        "x-edge-request-id",
        "x-host-header",
        "cs-protocol",
        "cs-bytes",
        "time-taken",
        "x-forwarded-for",
        "ssl-protocol",
        "ssl-cipher",
        "x-edge-response-result-type",
        "cs-protocol-version",
        "fle-status",
        "fle-encrypted-fields",
        "c-port",
        "time-to-first-byte",
        "x-edge-detailed-result-type",
        "sc-content-type",
        "sc-content-len",
        "sc-range-start",
        "sc-range-end",
        "c-country",
        "cache-behavior-path-pattern"
    ],
     "fieldDelimiter": ""
}
```

5. Depuis la CloudFront console, sur la page Logs, vérifiez que le statut standard des logs est Activé à côté de la distribution.

   Pour plus d'informations sur la livraison de la journalisation standard et les champs de journal, consultez la Référence de la journalisation standard.

> **Note**
>
> Pour activer la journalisation standard (v2) pour CloudFront en utilisant AWS CloudFormation, vous pouvez utiliser les propriétés de CloudWatch journalisation suivantes :
>
> - Delivery
> - DeliveryDestination
> - DeliverySource
>
> `ResourceArn`Il s'agit de la CloudFront distribution et `LogType` doit correspondre `ACCESS_LOGS` au type de journal pris en charge.

Activation de la journalisation standard pour la livraison entre comptes

Si vous activez la journalisation standard pour votre compte Compte AWS et que vous souhaitez transmettre vos journaux d'accès à un autre compte, assurez-vous de configurer correctement le compte source et le compte de destination. Le compte source associé à la CloudFront distribution envoie ses journaux d'accès au compte de destination.

Dans cet exemple de procédure, le *111111111111* (compte source) envoie ses journaux d'accès à un compartiment Amazon S3 du compte de destination (*222222222222*). Pour envoyer les journaux d’accès vers un compartiment Amazon S3 dans le compte de destination, utilisez l’ AWS CLI.

Configuration du compte de destination

Exécutez la procédure ci-dessous pour le compte de destination.

Pour configurer le compte de destination

1. Pour créer la destination de livraison des journaux, vous pouvez saisir la commande de l’ AWS CLI suivante. Cet exemple utilise la chaîne *MyLogPrefix* pour créer un préfixe pour vos journaux d’accès.

   ```
   aws logs put-delivery-destination --name cloudfront-delivery-destination --
   delivery-destination-configuration "destinationResourceArn=arn:aws:s3:::amzn-s3-
   demo-bucket-cloudfront-logs/MyLogPrefix"
   ```

   Sortie

```
{
    "deliveryDestination": {
        "name": "cloudfront-delivery-destination",
        "arn": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination",
        "deliveryDestinationType": "S3",
        "deliveryDestinationConfiguration": {"destinationResourceArn":
 "arn:aws:s3:::amzn-s3-demo-bucket-cloudfront-logs/MyLogPrefix"}
    }
}
```

> **Note**
>
> Si vous spécifiez un compartiment S3 sans préfixe, il CloudFront sera automatiquement ajouté en `AWSLogs/<account-ID>/CloudFront` tant que préfixe qui apparaît dans la destination `suffixPath` de livraison S3. Pour de plus amples informations, veuillez consulter S3DeliveryConfiguration.

2. Ajoutez la politique de ressource pour la destination de livraison des journaux afin d'autoriser le compte source à créer une livraison de journaux.

   Dans la politique suivante, remplacez-le *111111111111* par l'ID du compte source et spécifiez l'ARN de destination de livraison à partir de la sortie de l'étape 1.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateDelivery",
            "Effect": "Allow",
            "Principal": {"AWS": "111111111111"},
            "Action": ["logs:CreateDelivery"],
            "Resource": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination"
        }
    ]
}
```

3. Enregistrez le fichier, par exemple sous le nom `deliverypolicy.json`.
4. Pour associer la politique précédente à la destination de livraison, entrez la AWS CLI commande suivante.

```
aws logs put-delivery-destination-policy --delivery-destination-name cloudfront-delivery-destination --delivery-destination-policy file://deliverypolicy.json
```

5. Ajoutez l'instruction ci-dessous à la stratégie de compartiment Amazon S3 de destination, en remplaçant l'ARN de la ressource et l'ID du compte source. Cette stratégie autorise le principal de service `delivery.logs.amazonaws.com` à effectuer l'action `s3:PutObject`.

```
{
    "Sid": "AWSLogsDeliveryWrite",
    "Effect": "Allow",
    "Principal": {"Service": "delivery.logs.amazonaws.com"},
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-cloudfront-logs/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control",
            "aws:SourceAccount": "111111111111"
        },
        "ArnLike": {"aws:SourceArn": "arn:aws:logs:us-east-1:111111111111:delivery-source:*"}
    }
}
```

6. Si vous l'utilisez AWS KMS pour votre compartiment, ajoutez la déclaration suivante à la politique des clés KMS pour accorder des autorisations au principal du `delivery.logs.amazonaws.com` service.

```
{
    "Sid": "Allow Logs Delivery to use the key",
    "Effect": "Allow",
    "Principal": {"Service": "delivery.logs.amazonaws.com"},
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
```

```
    "Resource": "*",
    "Condition": {
        "StringEquals": {"aws:SourceAccount": "111111111111"},
        "ArnLike": {"aws:SourceArn": "arn:aws:logs:us-east-1:111111111111:delivery-
source:*"}
    }
}
```

Configuration du compte source

Une fois le compte de destination configuré, suivez cette procédure pour créer la source de livraison et activer la journalisation pour la distribution dans le compte source.

Pour configurer le compte source

1. Créez une source de diffusion pour la journalisation CloudFront standard afin de pouvoir envoyer des fichiers CloudWatch journaux à Logs.

   Vous pouvez entrer la AWS CLI commande suivante en remplaçant le nom et l'ARN de votre distribution.

   ```
   aws logs put-delivery-source --name s3-cf-delivery --resource-arn
    arn:aws:cloudfront::111111111111:distribution/E1TR1RHV123ABC --log-type
    ACCESS_LOGS
   ```

   Sortie

   ```
   {
       "deliverySource": {
           "name": "s3-cf-delivery",
           "arn": "arn:aws:logs:us-east-1:111111111111:delivery-source:s3-cf-
   delivery",
           "resourceArns":
    ["arn:aws:cloudfront::111111111111:distribution/E1TR1RHV123ABC"],
           "service": "cloudfront",
           "logType": "ACCESS_LOGS"
       }
   }
   ```

2. Créez une livraison pour associer la source de livraison des journaux du compte source à la destination de livraison des journaux du compte de destination.

Dans la AWS CLI commande suivante, spécifiez l'ARN de destination de livraison à partir de la sortie de l'étape 1 : Configurer le compte de destination.

```
aws logs create-delivery --delivery-source-name s3-cf-delivery --
delivery-destination-arn arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination
```

Sortie

```
{
    "delivery": {
        "id": "OPmOpLahVzhx1234",
        "arn": "arn:aws:logs:us-east-1:111111111111:delivery:OPmOpLahVzhx1234",
        "deliverySourceName": "s3-cf-delivery",
        "deliveryDestinationArn": "arn:aws:logs:us-east-1:222222222222:delivery-
destination:cloudfront-delivery-destination",
        "deliveryDestinationType": "S3",
        "recordFields": [
            "date",
            "time",
            "x-edge-location",
            "sc-bytes",
            "c-ip",
            "cs-method",
            "cs(Host)",
            "cs-uri-stem",
            "sc-status",
            "cs(Referer)",
            "cs(User-Agent)",
            "cs-uri-query",
            "cs(Cookie)",
            "x-edge-result-type",
            "x-edge-request-id",
            "x-host-header",
            "cs-protocol",
            "cs-bytes",
            "time-taken",
            "x-forwarded-for",
            "ssl-protocol",
            "ssl-cipher",
            "x-edge-response-result-type",
            "cs-protocol-version",
```

```
            "fle-status",
            "fle-encrypted-fields",
            "c-port",
            "time-to-first-byte",
            "x-edge-detailed-result-type",
            "sc-content-type",
            "sc-content-len",
            "sc-range-start",
            "sc-range-end",
            "c-country",
            "cache-behavior-path-pattern"
        ],
        "fieldDelimiter": "\t"
    }
}
```

3. Vérifiez que votre livraison entre comptes s'est déroulée correctement.

    a. Depuis le *source* compte, connectez-vous à la CloudFront console et choisissez votre distribution. Dans l'onglet Journalisation, la section Type affichera une entrée créée pour la livraison de journaux S3 entre comptes.

    b. Depuis le *destination* compte, connectez-vous à la console Amazon S3 et choisissez votre compartiment Amazon S3. Le préfixe *MyLogPrefix* apparaîtra dans le nom du compartiment et dans chaque journal d'accès livré dans ce dossier.

Format du fichier de sortie

En fonction de la destination de livraison que vous choisissez, vous pouvez spécifier l'un des formats suivants pour les fichiers journaux :

- JSON
- Plain
- w3c
- Raw
- Parquet (Amazon S3 uniquement)

> **Note**
>
> Vous ne pouvez définir le format de sortie que lorsque vous créez la destination de livraison pour la première fois. Cet élément ne peut pas être mis à jour ultérieurement. Pour modifier le format de sortie, supprimez la livraison et créez-en une autre.

Pour plus d'informations, consultez PutDeliveryDestinationle manuel Amazon CloudWatch Logs API Reference.

Modification des paramètres de journalisation standard

Vous pouvez activer ou désactiver la journalisation et mettre à jour d'autres paramètres de journalisation à l'aide de la CloudFront console ou de l' CloudWatch API. Les modifications apportées aux paramètres de journalisation prennent effet dans les 12 heures.

Pour plus d’informations, consultez les rubriques suivantes :

- Pour mettre à jour une distribution à l'aide de la CloudFront console, consultezMettre à jour une distribution.
- Pour mettre à jour une distribution à l'aide de l' CloudFront API, consultez UpdateDistributionle Amazon CloudFront API Reference.
- Pour plus d'informations sur CloudWatch les opérations de l'API Logs, consultez le manuel Amazon CloudWatch Logs API Reference.

Accès aux champs de journal

Vous pouvez sélectionner les mêmes champs de journal que ceux pris en charge par la journalisation standard (héritée). Pour plus d’informations, consultez Champs d’un fichier journal.

En outre, vous pouvez sélectionner les champs du journal d'accès en temps réel suivants.

1. **`timestamp(ms)`** : horodatage en millisecondes.
2. **`origin-fbl`**— Le nombre de secondes de latence du premier octet entre CloudFront et votre origine.
3. **`origin-lbl`**— Le nombre de secondes de latence du dernier octet entre CloudFront et votre origine.

4. **`asn`** : le numéro de système autonome (ASN) de l'utilisateur.
5. **`c-country`** : un code de pays qui représente l'emplacement géographique de l'utilisateur, déterminé par l'adresse IP de l'utilisateur. Pour obtenir une liste des codes de pays, consultez ISO 3166-1 alpha-2.
6. **`cache-behavior-path-pattern`** : le modèle de chemin qui identifie le comportement du cache correspondant à la demande de l'utilisateur.
7. **`viewer-request-log-data`**— Contient les données personnalisées que votre CloudFront fonction de demande de visualisation envoie à l'aide de la méthode d'`cf.logCustomData()`assistance. CloudFront URL-encodes la valeur et la tronque à un maximum de 800 octets. Si aucune CloudFront fonction n'est associée à l'événement de demande du spectateur, ou si la fonction n'appelle pas`cf.logCustomData()`, ce champ est défini comme tel`-`. Pour de plus amples informations, veuillez consulter Méthodes d'assistance générales.
8. **`viewer-response-log-data`**— Contient les données personnalisées que votre CloudFront fonction de réponse du spectateur envoie à l'aide de la méthode d'`cf.logCustomData()`assistance. CloudFront URL-encodes la valeur et la tronque à un maximum de 800 octets. Si aucune CloudFront fonction n'est associée à l'événement de réponse du spectateur, ou si la fonction n'appelle pas`cf.logCustomData()`, ce champ est défini comme tel`-`. Pour de plus amples informations, veuillez consulter Méthodes d'assistance générales.

Envoyer des journaux à CloudWatch Logs

Pour envoyer des CloudWatch journaux à Logs, créez ou utilisez un groupe de CloudWatch journaux Logs existant. Pour plus d'informations sur la configuration d'un groupe de CloudWatch journaux, consultez la section Utilisation des groupes de journaux et des flux de journaux.

Après avoir créé votre groupe de journaux, vous devez disposer des autorisations nécessaires pour activer la journalisation standard. Pour plus d'informations sur les autorisations requises, consultez la section Logs envoyés à CloudWatch Logs dans le guide de l'utilisateur Amazon CloudWatch Logs.

> **Remarques**
>
> - Lorsque vous spécifiez le nom du groupe de CloudWatch journaux Logs, utilisez uniquement le modèle `[\w-]` regex. Pour plus d'informations, consultez le fonctionnement de l'PutDeliveryDestinationAPI dans le manuel Amazon CloudWatch Logs API Reference.
> - Vérifiez que la politique de ressources de votre groupe de journaux ne dépasse pas la limite de taille autorisée. Consultez la section Considérations relatives à la limite de taille

des ressources liées à la politique des groupes de CloudWatch journaux dans la rubrique Journaux.

Exemple de journal d'accès envoyé à CloudWatch Logs

```
{
"date": "2024-11-14",
"time": "21:34:06",
"x-edge-location": "SOF50-P2",
"asn": "16509",
"timestamp(ms)": "1731620046814",
"origin-fbl": "0.251",
"origin-lbl": "0.251",
"x-host-header": "d111111abcdef8.cloudfront.net",
"cs(Cookie)": "examplecookie=value"
}
```

Envoi des journaux à Firehose

Pour envoyer des journaux à Firehose, créez ou utilisez un flux de diffusion Firehose existant. Indiquez ensuite le flux de diffusion Firehose comme destination de livraison des journaux. Vous devez indiquer un flux de diffusion Firehose situé dans la région USA Est (Virginie du Nord).

Pour en savoir plus sur la création des flux de diffusion, consultez Création d'un flux de diffusion Amazon Data Firehose.

Après avoir créé votre flux de diffusion, vous devez disposer des autorisations nécessaires pour activer la journalisation standard. Pour plus d'informations, consultez la section Logs envoyés à Firehose dans le guide de l'utilisateur Amazon CloudWatch Logs.

> **Note**
>
> Lorsque vous indiquez le nom du flux Firehose, utilisez uniquement le modèle regex `[\w-]`. Pour plus d'informations, consultez le fonctionnement de l'PutDeliveryDestinationAPI dans le manuel Amazon CloudWatch Logs API Reference.

Exemple de journal d’accès envoyé à Firehose


```
{"date":"2024-11-15","time":"19:45:51","x-edge-location":"SOF50-
P2","asn":"16509","timestamp(ms)":"1731699951183","origin-fbl":"0.254","origin-
lbl":"0.254","x-host-
header":"d111111abcdef8.cloudfront.net","cs(Cookie)":"examplecookie=value"}
{"date":"2024-11-15","time":"19:45:52","x-edge-location":"SOF50-
P2","asn":"16509","timestamp(ms)":"1731699952950","origin-fbl":"0.125","origin-
lbl":"0.125","x-host-
header":"d111111abcdef8.cloudfront.net","cs(Cookie)":"examplecookie=value"}
```


Envoi de journaux vers Amazon S3

Pour envoyer vos journaux d’accès à Amazon S3, créez ou utilisez un compartiment S3 existant. Lorsque vous activez la connexion CloudFront, spécifiez le nom du compartiment. Pour en savoir plus sur la création des compartiments, consultez Création d’un compartiment dans le Guide de l’utilisateur Amazon Simple Storage Service.

Une fois votre compartiment créé, vous devez disposer des autorisations nécessaires pour activer la journalisation standard. Pour plus d'informations, consultez la section Logs envoyés à Amazon S3 dans le guide de l'utilisateur Amazon CloudWatch Logs.

- Une fois que vous avez activé la journalisation, il ajoute AWS automatiquement les politiques de compartiment requises pour vous.
- Vous pouvez également utiliser des compartiments S3 dans les Régions AWS soumises à adhésion.

> **Note**
>
> Si vous utilisez déjà la journalisation standard (héritée) et que vous souhaitez activer la journalisation standard (v2) sur Amazon S3, nous vous conseillons d’indiquer un compartiment Amazon S3 différent ou d’utiliser un chemin distinct dans le même compartiment (par exemple, un préfixe de journal ou un partitionnement). Vous pouvez ainsi facilement identifier les fichiers journaux associés à chaque distribution, tout en évitant qu’ils ne se remplacent mutuellement.

Rubriques

- Spécification d’un compartiment S3

- Partitioning
- Hive-compatible format de nom de fichier
- Exemple de chemins d’accès aux journaux
- Exemple de journal d’accès envoyé à Amazon S3

Spécification d’un compartiment S3

Lorsque vous spécifiez un compartiment S3 comme destination de livraison, tenez compte des points suivants.

Le nom du compartiment S3 ne peut utiliser que le modèle regex `[\w-]`. Pour plus d'informations, consultez le fonctionnement de l'PutDeliveryDestinationAPI dans le manuel Amazon CloudWatch Logs API Reference.

Si vous avez spécifié un préfixe pour votre compartiment S3, vos journaux seront visibles sous ce chemin. Si vous ne spécifiez aucun préfixe, CloudFront il sera automatiquement ajouté pour `AWSLogs/{account-id}/CloudFront` vous.

Pour de plus amples informations, veuillez consulter Exemple de chemins d’accès aux journaux.

Partitioning

Vous pouvez utiliser le partitionnement pour organiser vos journaux d'accès lorsque vous CloudFront les envoyez à votre compartiment S3. Cela vous permet d’organiser et de localiser vos journaux d’accès en fonction du chemin souhaité.

Vous pouvez utiliser les variables suivantes pour créer un chemin de dossier.

- `{DistributionId}` ou `{distributionid}`
- `{yyyy}`
- `{MM}`
- `{dd}`
- `{HH}`
- `{accountid}`

Vous pouvez utiliser autant de variables que vous le souhaitez et spécifier des noms de dossiers dans votre chemin. CloudFrontutilise ensuite ce chemin pour créer une structure de dossiers pour vous dans le compartiment S3.

Exemples

- *my_distribution_log_data*/{DistributionId}/*logs*
- /*cloudfront*/{DistributionId}/*my_distribution_log_data*/{yyyy}/{MM}/{dd}/{HH}/*logs*

> **Note**
>
> Vous pouvez utiliser l'une ou l'autre variable pour l'ID de distribution dans le chemin de suffixe. Toutefois, si vous envoyez des journaux d'accès à AWS Glue, vous devez utiliser la {distributionid} variable car AWS Glue les noms de partition doivent être en minuscules. Mettez à jour votre configuration de journal existante CloudFront pour la {DistributionId} remplacer par{distributionid}.

Hive-compatible format de nom de fichier

Cette option peut être utilisée afin que les objets S3 contenant les journaux d'accès livrés utilisent une structure de préfixe permettant l'intégration avec Apache Hive. Pour plus d'informations, consultez l'opération API CreateDelivery.

Example Exemple

```
/cloudfront/DistributionId={DistributionId}/my_distribution_log_data/year={yyyy}/
month={MM}/day={dd}/hour={HH}/logs
```

Pour plus d'informations sur le partitionnement et les Hive-compatible options, consultez l'S3DeliveryConfigurationélément dans le manuel Amazon CloudWatch Logs API Reference.

Exemple de chemins d'accès aux journaux

Lorsque vous spécifiez un compartiment S3 comme destination, vous pouvez utiliser les options suivantes pour créer le chemin d'accès à vos journaux d'accès :

- Un compartiment Amazon S3, avec ou sans préfixe
- Partitionnement, en utilisant une variable CloudFront fournie ou en saisissant la vôtre
- Activation de l' Hive-compatible option

Les tableaux suivants montrent comment vos journaux d'accès apparaissent dans votre compartiment, en fonction des options que vous avez choisies.

Compartiment Amazon S3 avec un préfixe

Nom du compartiment Amazon S3	Partition que vous spécifiez dans le chemin du suffixe	Chemin de suffixe mis à jour	Hive-compatible activé ?	Les journaux d'accès sont envoyés à
`amzn-s3-demo-bucket/MyLogPrefix`	Aucune	Aucune	Non	`amzn-s3-demo-bucket/MyLogPrefix/`
`amzn-s3-demo-bucket/MyLogPrefix`	`myFolderA/`	`myFolderA/`	Non	`amzn-s3-demo-bucket/MyLogPrefix/myFolderA/`
`amzn-s3-demo-bucket/MyLogPrefix`	`myFolderA/{yyyy}`	`myFolderA/{yyyy}`	Oui	`amzn-s3-demo-bucket/MyLogPrefix/myFolderA/year=2025`

Compartiment Amazon S3 sans préfixe

Nom du compartiment Amazon S3	Partition que vous spécifiez dans le chemin du suffixe	Chemin de suffixe mis à jour	Hive-compatible activé ?	Les journaux d'accès sont envoyés à
`amzn-s3-demo-bucket`	Aucune	`AWSLogs/{account-i`	Non	`amzn-s3-demo-bucke`

Nom du compartiment Amazon S3	Partition que vous spécifiez dans le chemin du suffixe	Chemin de suffixe mis à jour	Hive-compatible activé ?	Les journaux d'accès sont envoyés à
		d}/CloudFront/		t/AWSLogs/ *<your-account-ID>* /CloudFront/
amzn-s3-demo-bucket	myFolderA/	AWSLogs/{account-id}/CloudFront/myFolderA/	Non	amzn-s3-demo-bucket/AWSLogs/ *<your-account-ID>* /CloudFront/myFolderA/
amzn-s3-demo-bucket	myFolderA/	AWSLogs/{account-id}/CloudFront/myFolderA/	Oui	amzn-s3-demo-bucket/AWSLogs/aws-account-id=*<your-account-ID>* /CloudFront/myFolderA/

Nom du compartiment Amazon S3	Partition que vous spécifiez dans le chemin du suffixe	Chemin de suffixe mis à jour	Hive-compatible activé ?	Les journaux d'accès sont envoyés à
amzn-s3-demo-bucket	myFolderA/{yyyy}	AWSLogs/{account-id}/CloudFront/myFolderA/{yyyy}	Oui	amzn-s3-demo-bucket/AWSLogs/aws-account-id=*<your-account-ID>* /CloudFront/myFolderA/year=2025

Compte AWS ID en tant que partition

Nom du compartiment Amazon S3	Partition que vous spécifiez dans le chemin du suffixe	Chemin de suffixe mis à jour	Hive-compatible activé ?	Les journaux d'accès sont envoyés à
amzn-s3-demo-bucket	Aucune	AWSLogs/{account-id}/CloudFront/	Oui	amzn-s3-demo-bucket/AWSLogs/aws-account-id=*<your-account-ID>* /CloudFront/
amzn-s3-demo-bucket	myFolderA/{accountid}	AWSLogs/{account-id}/CloudFront/myFo	Oui	amzn-s3-demo-bucket/AWSLogs/aws-

Nom du compartiment Amazon S3	Partition que vous spécifiez dans le chemin du suffixe	Chemin de suffixe mis à jour	Hive-compatible activé ?	Les journaux d'accès sont envoyés à
		`lderA/{accountid}`		`account-id=<your-account-ID>/CloudFront/myFolderA/accountid= <your-account-ID>`

> **Remarques**
>
> - La `{account-id}` variable est réservée à CloudFront. CloudFrontajoute automatiquement cette variable au chemin de votre suffixe si vous spécifiez un compartiment Amazon S3 sans préfixe. Si vos journaux le sont Hive-compatible, cette variable apparaît sous la forme`aws-account-id`.
> - Vous pouvez utiliser la `{accountid}` variable pour CloudFront ajouter votre identifiant de compte au chemin du suffixe. Si vos journaux le sont Hive-compatible, cette variable apparaît sous la forme`accountid`.
> - Pour plus d'informations sur le chemin du suffixe, consultez S3DeliveryConfiguration.

Exemple de journal d'accès envoyé à Amazon S3

```
#Fields: date time x-edge-location asn timestamp(ms) x-host-header cs(Cookie)
2024-11-14    22:30:25    SOF50-P2    16509    1731623425421
d111111abcdef8.cloudfront.net    examplecookie=value2
```

Désactivation de la journalisation standard

Si vous n'avez plus besoin de la journalisation standard, vous pouvez la désactiver sur votre distribution.

Pour désactiver la journalisation standard

1. Connectez-vous à la CloudFront console.
2. Sélectionnez Distribution, puis choisissez votre ID de distribution.
3. Choisissez Logging, puis sous Destinations du journal d'accès, sélectionnez la destination.
4. Sélectionnez Gérer, puis choisissez Supprimer.
5. Répétez l'étape précédente si vous avez plus d'une journalisation standard.

> **Note**
>
> Lorsque vous supprimez la journalisation standard de la CloudFront console, cette action supprime uniquement la livraison et la destination de livraison. Cela ne supprime pas la source de diffusion de votre Compte AWS. Pour supprimer une source de livraison, spécifiez le nom de la source de livraison dans la commande `aws logs delete-delivery-source --name DeliverySourceName`. Pour plus d'informations, consultez DeleteDeliverySourcele manuel Amazon CloudWatch Logs API Reference.

Dépannage

Utilisez les informations suivantes pour résoudre les problèmes courants liés à l'utilisation de la journalisation CloudFront standard (v2).

La source de livraison existe déjà

Lorsque vous activez la journalisation standard pour une distribution, vous créez une source de livraison. Vous utilisez ensuite cette source de livraison pour créer des livraisons vers le type de destination que vous souhaitez : CloudWatch Logs, Firehose, Amazon S3. À l'heure actuelle, une distribution ne peut disposer que d'une seule source de livraison. Si vous essayez de créer une autre source de livraison pour la même distribution, le message d'erreur suivant s'affiche.

```
This ResourceId has already been used in another Delivery Source in this account
```

Pour créer une autre source de livraison, supprimez d'abord la source existante. Pour plus d'informations, consultez DeleteDeliverySourcele manuel Amazon CloudWatch Logs API Reference.

J’ai modifié le chemin du suffixe et le compartiment Amazon S3 ne parvient plus à recevoir mes journaux

Si vous avez activé la journalisation standard (v2) et que vous spécifiez un ARN de compartiment sans préfixe, CloudFront vous ajouterez la valeur par défaut suivante au chemin du suffixe :. `AWSLogs/{account-id}/CloudFront` Si vous utilisez la CloudFront console ou l'opération UpdateDeliveryConfigurationAPI pour spécifier un chemin de suffixe différent, vous devez mettre à jour la politique du compartiment Amazon S3 pour utiliser le même chemin.

Example Exemple : mise à jour du chemin de suffixe

1. Votre chemin de suffixe par défaut est `AWSLogs/{account-id}/CloudFront` et vous le remplacez par `myFolderA`.
2. Étant donné que votre nouveau chemin de suffixe diffère de celui indiqué dans la stratégie de compartiment Amazon S3, vos journaux d’accès ne seront pas livrés.
3. Vous pouvez effectuer l’une des actions suivantes :
   - Mettre à jour l’autorisation du compartiment Amazon S3 en remplaçant `amzn-s3-demo-bucket/AWSLogs/<your-account-ID>/CloudFront/*` par `amzn-s3-demo-bucket/myFolderA/*`.
   - Mettre à jour votre configuration de journalisation pour réutiliser le chemin de suffixe par défaut : `AWSLogs/{account-id}/CloudFront`

Pour plus d’informations, consultez Permissions.

Suppression des fichiers journaux

CloudFront ne supprime pas automatiquement les fichiers journaux de votre destination. Pour en savoir plus sur la suppression des fichiers journaux, consultez les rubriques suivantes :

Amazon S3

- Suppression des objets dans le Guide de l’utilisateur de la console Amazon Simple Storage Service

CloudWatch Journaux

- Utilisation des groupes de journaux et des flux de journaux dans le guide de l'utilisateur Amazon CloudWatch Logs

- DeleteLogGroupdans le manuel de référence de l'API Amazon CloudWatch Logs

Firehose

- DeleteDeliveryStreamdans le manuel de référence de l'API Amazon Data Firehose

Tarification

CloudFront l'activation des journaux standard n'est pas facturée. Cependant, vous pouvez être facturé pour la livraison, l’ingestion, le stockage ou l’accès, selon la destination de livraison des journaux que vous avez choisie. Pour plus d'informations, consultez la section Tarification d'Amazon CloudWatch Logs. Dans Niveau payant, sélectionnez l’onglet Journaux, puis, dans Journaux payants, consultez les informations pour chaque destination de livraison.

Pour plus d'informations sur la tarification de chacun d'entre eux Service AWS, consultez les rubriques suivantes :

- Tarification d'Amazon CloudWatch Logs
- Tarification Amazon Data Firehose
- Tarification Amazon S3

> **Note**
>
> La livraison des journaux vers Amazon S3 n’entraîne aucun coût supplémentaire, toutefois vous serez facturé par Amazon S3 pour le stockage et l’accès aux fichiers journaux. Si vous activez l'option Parquet pour convertir vos journaux d'accès en Apache Parquet, cette option entraîne des CloudWatch frais. Pour plus d'informations, consultez la section Vended Logs pour CloudWatch connaître les tarifs.

Configurer la journalisation standard (héritée)

> **Remarques**
>
> - Cette rubrique concerne la version précédente de la journalisation standard. Pour obtenir la dernière version, consultez Configuration de la journalisation standard (v2).

- Si vous utilisez déjà la journalisation standard (héritée) et que vous souhaitez activer la journalisation standard (v2) sur Amazon S3, nous vous conseillons d'indiquer un compartiment Amazon S3 différent ou d'utiliser un chemin distinct dans le même compartiment (par exemple, un préfixe de journal ou un partitionnement). Vous pouvez ainsi facilement identifier les fichiers journaux associés à chaque distribution, tout en évitant qu'ils ne se remplacent mutuellement.

Pour commencer avec la journalisation standard (héritée), procédez comme suit :

1. Choisissez un compartiment Amazon S3 qui recevra vos journaux, puis ajoutez les autorisations requises.
2. Configurez la journalisation standard (ancienne) depuis la CloudFront console ou l' CloudFront API. Vous ne pouvez choisir qu'un compartiment Amazon S3 pour recevoir vos journaux.
3. Affichez vos journaux d'accès.

Choix d'un compartiment Amazon S3 pour les journaux standard

Lorsque vous activez la journalisation pour une distribution, vous spécifiez le compartiment Amazon S3 dans lequel vous CloudFront souhaitez stocker les fichiers journaux. Si vous utilisez Amazon S3 comme origine, nous vous recommandons d'utiliser un compartiment distinct pour vos fichiers journaux.

Spécifiez le compartiment Amazon S3 dans lequel vous CloudFront souhaitez stocker les journaux d'accès, par exemple`amzn-s3-demo-bucket.s3.amazonaws.com`.

Vous pouvez stocker les fichiers journaux de plusieurs distributions dans le même compartiment. Lorsque vous activez la journalisation, vous pouvez spécifier un préfixe facultatif pour les noms de fichier et vous pouvez ainsi savoir quels fichiers journaux sont associés à quelles distributions.

À propos du choix d'un compartiment S3

- La liste de contrôle d'accès (ACL) doit être activée sur votre compartiment. Si vous choisissez un bucket sans ACL activée depuis la CloudFront console, un message d'erreur s'affiche. Consultez Permissions.
- Ne choisissez pas un compartiment Amazon S3 avec l'option S3 Object Ownership (Propriété de l'objet S3) définie sur bucket owner enforced (appliqué par le propriétaire du

compartiment). Ce paramètre désactive les ACL pour le compartiment et les objets qu'il contient, ce qui CloudFront empêche la livraison de fichiers journaux au compartiment.

- L'ancienne journalisation ne prend pas en charge les compartiments Amazon S3 dans les régions optionnelles. Choisissez une région activée par défaut ou utilisez Standard Logging V2 qui prend en charge les régions optionnelles et des fonctionnalités supplémentaires. Pour obtenir la liste des régions par défaut et facultatives, consultez Régions AWS.

Permissions

Important

À compter d'avril 2023, vous devez activer les ACL S3 pour les nouveaux compartiments S3 utilisés pour les journaux CloudFront standard. Vous pouvez activer les ACL lorsque vous créez un compartiment ou activer les ACL pour un compartiment existant.
Pour plus d'informations sur les modifications, consultez la FAQ sur les paramètres par défaut pour les nouveaux compartiments S3 dans le Guide de l'utilisateur d'Amazon Simple Storage Service et Heads-Up : Les modifications de sécurité d'Amazon S3 arriveront en avril 2023 dans le AWS News Blog.

Vous Compte AWS devez disposer des autorisations suivantes pour le compartiment que vous spécifiez pour les fichiers journaux :

- L'ACL définie pour le compartiment doit vous accorder l'autorisation `FULL_CONTROL`. Si vous êtes le propriétaire du compartiment, votre compte dispose de cette autorisation par défaut. Si vous ne l'êtes pas, le propriétaire du compartiment doit mettre à jour l'ACL de ce compartiment.
- `s3:GetBucketAcl`
- `s3:PutBucketAcl`

Liste ACL pour le compartiment

Lorsque vous créez ou mettez à jour une distribution et que vous activez la journalisation, CloudFront utilise ces autorisations pour mettre à jour l'ACL du bucket afin de donner l'`FULL_CONTROL`autorisation au `awslogsdelivery` compte. Le compte `awslogsdelivery`

écrit les fichiers journaux dans le compartiment. Si votre compte ne dispose pas des autorisations requises pour mettre à jour la liste ACL, la création ou la mise à jour de la distribution échouera.

Dans certaines circonstances, si vous envoyez par programmation une demande pour créer un compartiment, mais qu'un compartiment avec le nom spécifié existe déjà, S3 réinitialise les autorisations sur le compartiment à la valeur par défaut. Si vous avez configuré CloudFront pour enregistrer les journaux d'accès dans un compartiment S3 et que vous ne recevez plus de journaux dans ce compartiment, vérifiez les autorisations sur le compartiment pour vous assurer qu'il CloudFront dispose des autorisations nécessaires.

Restauration de la liste ACL pour le compartiment

Si vous supprimez des autorisations pour le compte `awslogsdelivery`, CloudFront ne peut plus enregistrer des journaux dans le compartiment S3. Pour recommencer CloudFront à enregistrer les journaux de votre distribution, restaurez l'autorisation ACL en effectuant l'une des opérations suivantes :

- Désactivez la journalisation de votre distribution dans CloudFront, puis réactivez-la. Pour plus d'informations, consultez Journalisation standard.
- Ajoutez manuellement l'autorisation de la liste ACL pour le compte `awslogsdelivery` en accédant au compartiment S3 dans la console Amazon S3 et en ajoutant l'autorisation. Afin d'ajouter la liste ACL pour le compte `awslogsdelivery`, vous devez fournir l'ID canonique suivant pour le compte :

  ```
  c4c1ede66af53448b93c283ce9448c4ba468c9432aa01d700d3878632f77d2d0
  ```

  Pour plus d'informations sur l'ajout d'ACL aux compartiments S3, consultez Configuration des listes ACL dans le Guide de l'utilisateur Amazon Simple Storage Service.

Liste ACL pour chaque fichier journal

En plus de la liste ACL sur le compartiment, il existe une ACL sur chaque fichier journal. Le propriétaire du compartiment dispose de l'autorisation `FULL_CONTROL` sur chaque fichier journal, le propriétaire de la distribution (s'il est différent du propriétaire du compartiment) n'a aucune autorisation et le compte `awslogsdelivery` a les autorisations en lecture et écriture.

Désactivation de la journalisation

Si vous désactivez la journalisation, CloudFront cela ne supprime pas les ACL du bucket ou des fichiers journaux. Vous pouvez supprimer les ACL si nécessaire.

Politique clé requise pour les SSE-KMS compartiments

Si le compartiment S3 de vos journaux standard utilise un chiffrement côté serveur avec AWS KMS keys (SSE-KMS) à l'aide d'une clé gérée par le client, vous devez ajouter l'instruction suivante à la politique de clé pour votre clé gérée par le client. Cela permet CloudFront d'écrire des fichiers journaux dans le bucket. Vous ne pouvez pas SSE-KMS l'utiliser Clé gérée par AWS car vous CloudFront ne pourrez pas écrire de fichiers journaux dans le compartiment.

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Si le compartiment S3 pour vos journaux standard est utilisé SSE-KMS avec une clé de compartiment S3, vous devez également ajouter l'`kms:Decrypt`autorisation à la déclaration de politique. Dans ce cas, l'énoncé de stratégie complet ressemble à ce qui suit.

```
{
    "Sid": "Allow CloudFront to use the key to deliver logs",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

> **Note**
>
> Lorsque vous activez SSE-KMS votre compartiment S3, spécifiez l'ARN complet de la clé gérée par le client. Pour plus d'informations, consultez la section Spécifier le chiffrement côté

serveur avec AWS KMS keys (SSE-KMS) dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

Activation de la journalisation standard (héritée)

Pour activer les journaux standard, utilisez la CloudFront console ou l' CloudFront API.

Table des matières

- Activer la journalisation standard (ancienne) (CloudFront console)
- Activer la journalisation standard (ancienne) (CloudFront API)

Activer la journalisation standard (ancienne) (CloudFront console)

Pour activer les journaux standard pour une CloudFront distribution (console)

1. Utilisez la CloudFront console pour créer une nouvelle distribution ou mettre à jour une distribution existante.
2. Dans la section Journalisation standard, sélectionnez Activé pour la Livraison des journaux.
3. (Facultatif) Pour la journalisation des cookies, choisissez Activé si vous souhaitez inclure les cookies dans vos journaux. Pour plus d'informations, consultez Journalisation des cookies.

   > **Tip**
   >
   > La journalisation des cookies est un paramètre global qui s'applique à l'ensemble des journaux standard de votre distribution. Vous ne pouvez pas remplacer ce paramètre pour des destinations de livraison distinctes.

4. Dans la section Livrer à, indiquez Amazon S3 (hérité).
5. Indiquez votre compartiment Amazon S3. Si vous n'en avez pas encore, vous pouvez choisir Créer ou consulter la documentation pour créer un compartiment.
6. (Facultatif) Pour Préfixe du journal, spécifiez la chaîne, le cas échéant, que vous CloudFront souhaitez ajouter au préfixe des noms de fichiers journaux d'accès pour cette distribution, par exemple. `exampleprefix/` La barre oblique de fin (/) est facultative, mais recommandée pour simplifier la navigation dans vos fichiers-journaux. Pour plus d'informations, consultez Préfixe de journal.

7. Terminez les étapes pour mettre à jour ou créer votre distribution.
8. Sur la page Journaux, vérifiez que l'état des journaux standard est défini sur Activé à côté de la distribution.

   Pour plus d'informations sur la livraison de la journalisation standard et les champs de journal, consultez la Référence de la journalisation standard.

Activer la journalisation standard (ancienne) (CloudFront API)

Vous pouvez également utiliser l' CloudFront API pour activer les journaux standard pour vos distributions.

Pour activer les journaux standard pour une distribution (CloudFront API)

- Utilisez l'opération UpdateDistribution d'API CreateDistribution or et configurez l'LoggingConfigobjet.

Modification des paramètres de journalisation standard

Vous pouvez activer ou désactiver la journalisation, modifier le compartiment Amazon S3 dans lequel vos journaux sont stockés et modifier le préfixe des fichiers journaux à l'aide de la CloudFront console ou de l' CloudFront API. Les modifications apportées aux paramètres de journalisation prennent effet dans les 12 heures.

Pour plus d'informations, consultez les rubriques suivantes :

- Pour mettre à jour une distribution à l'aide de la CloudFront console, consultezMettre à jour une distribution.
- Pour mettre à jour une distribution à l'aide de l' CloudFront API, consultez UpdateDistribution le manuel Amazon CloudFront API Reference.

Envoi de journaux vers Amazon S3

Lorsque vos journaux sont envoyés à Amazon S3, ils se présentent sous le format suivant.

Format de nom de fichier

Le nom de chaque fichier journal enregistré CloudFront dans votre compartiment Amazon S3 utilise le format de nom de fichier suivant :

<optional prefix>/*<distribution ID>*.*YYYY*-*MM*-*DD*-*HH*.*unique-ID*.gz

Les dates et heures sont exprimées en heure UTC (temps universel coordonné).

Par exemple, si vous utilisez `example-prefix` comme préfixe et que votre ID de distribution est `EMLARXS9EXAMPLE`, les noms de fichiers ressemblent à ceci :

```
example-prefix/EMLARXS9EXAMPLE.2019-11-14-20.RT4KCN4SGK9.gz
```

Lorsque vous activez la journalisation pour une distribution, vous pouvez spécifier un préfixe facultatif pour les noms de fichier et vous pouvez ainsi savoir quels fichiers journaux sont associés à quelles distributions. Si vous incluez une valeur pour le préfixe du fichier journal et que celui-ci ne se termine pas par une barre oblique (/), une barre oblique () en CloudFront ajoute une automatiquement. Si votre préfixe se termine par une barre oblique, CloudFront il n'en ajoute pas d'autre.

Le symbole `.gz` à la fin du nom de fichier indique que le fichier journal CloudFront a été compressé à l'aide de gzip.

Format de fichier journal standard

Chaque entrée d'un fichier journal fournit des informations détaillées sur une seule demande utilisateur. Les fichiers journaux présentent les caractéristiques suivantes :

- Utilisez le format de fichier journal étendu W3C.
- Contiennent des valeurs séparées par des virgules.
- Contiennent des enregistrements qui ne sont pas nécessairement dans l'ordre chronologique.
- Contiennent deux lignes d'en-tête : l'une avec la version fichier-format et l'autre qui répertorie les champs W3C inclus dans chaque enregistrement.
- Contient des URL-encoded équivalents pour les espaces et certains autres caractères dans les valeurs des champs.

  URL-encoded des équivalents sont utilisés pour les caractères suivants :

  - Codes de caractères ASCII 0 à 32 inclus
  - Codes de caractères ASCII 127 et suivants
  - Tous les caractères du tableau suivant

  La norme d'encodage d'URL est définie dans la norme RFC 1738.

URL-Encoded valeur	Caractère
%3C	<
%3E	>
%22	"
%23	#
%25	%
%7B	{
%7D	}
%7C	|
%5C	\
%5E	^
%7E	~
%5B	[
%5D	]
%60	`
%27	'
%20	espace

Suppression des fichiers journaux

CloudFront ne supprime pas automatiquement les fichiers journaux de votre compartiment Amazon S3. Pour en savoir plus sur la suppression de fichiers journaux dans un compartiment Amazon S3, consultez Suppression des objets dans le Guide de l'utilisateur de la console Amazon Simple Storage Service.

Tarification

La journalisation standard est une fonctionnalité optionnelle de CloudFront. CloudFront l'activation des journaux standard est gratuite. Cependant, les frais Amazon S3 usuels sont facturés pour stocker les fichiers et y accéder sur Amazon S3. Vous pouvez les supprimer à tout moment.

Pour plus d’informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

Pour plus d'informations sur la CloudFront tarification, consultez la section CloudFront Tarification.

Référence de la journalisation standard

Les sections suivantes s’appliquent à la fois à la journalisation standard (v2) et à la journalisation standard (héritée).

Rubriques

- Chronologie de la livraison des fichiers journaux
- Comment les demandes sont consignées lorsque l’URL de la demande ou les en-têtes dépassent la taille maximale
- Champs du fichier journal
- Analyse des journaux

Chronologie de la livraison des fichiers journaux

CloudFront livre des grumes pour une distribution jusqu'à plusieurs fois par heure. En général, un fichier journal contient des informations sur les demandes CloudFront reçues au cours d'une période donnée. CloudFront envoie généralement le fichier journal pour cette période à votre destination dans l'heure qui suit les événements qui apparaissent dans le journal. Notez, cependant, que tout ou partie des entrées d’un fichier journal d’une période peut parfois être retardé de 24 heures au plus. Lorsque les entrées du journal sont retardées, les CloudFront enregistre dans un fichier journal dont le nom de fichier inclut la date et l'heure de la période au cours de laquelle les demandes ont été effectuées, et non la date et l'heure de livraison du fichier.

Lors de la création d'un fichier journal, CloudFront consolide les informations relatives à votre distribution provenant de tous les emplacements périphériques qui ont reçu des demandes pour vos objets au cours de la période couverte par le fichier journal.

CloudFront peut enregistrer plusieurs fichiers pendant une période donnée en fonction du nombre de demandes CloudFront reçues pour les objets associés à une distribution.

CloudFront commence à fournir des journaux d'accès de manière fiable environ quatre heures après l'activation de la journalisation. Vous pourriez obtenir quelques journaux d'accès avant ce moment-là.

> **Note**
>
> Si aucun utilisateur ne demande vos objets pendant la période, vous ne recevez aucun fichier journal pour cette dernière.

Comment les demandes sont consignées lorsque l'URL de la demande ou les en-têtes dépassent la taille maximale

Si la taille totale de tous les en-têtes de demande, y compris les cookies, dépasse 20 Ko ou si l'URL de demande dépasse les 8 192 octets pour l'URL, CloudFront ne peut pas analyser complètement la demande et ne peut pas la consigner. Étant donné que la demande n'est pas consignée, vous ne verrez pas dans les fichiers journaux le code de statut d'erreur HTTP renvoyé.

Si le corps de la demande dépasse la taille maximale, la demande est consignée, y compris le code de statut d'erreur HTTP.

Champs du fichier journal

Le fichier journal d'une distribution contient 33 champs. La liste suivante contient chaque nom de champ, dans l'ordre, ainsi qu'une description des informations contenues dans ce champ.

1. **`date`**

   Date à laquelle l'événement s'est produit au format `YYYY-MM-DD`. Par exemple : `2019-06-30`. Les dates et heures sont exprimées en heure UTC (temps universel coordonné). Pour les WebSocket connexions, il s'agit de la date de fermeture de la connexion.
2. **`time`**

   Heure à laquelle le CloudFront serveur a fini de répondre à la demande (en UTC), par exemple`01:42:39`. Pour les WebSocket connexions, il s'agit de l'heure à laquelle la connexion est fermée.
3. **`x-edge-location`**

   Emplacement périphérique ayant servi la demande. Chaque emplacement périphérique est identifié par un code à trois lettres et un numéro attribué arbitrairement (par exemple, DFW3). Le code à trois lettres correspond généralement au code IATA (International Air Transport

Association) d'un aéroport proche de l'emplacement périphérique. (Ces abréviations peuvent changer à l'avenir.)

4. **`sc-bytes`**

   Nombre total d'octets envoyés par le serveur à l'utilisateur en réponse à la demande, en-têtes inclus. Pour les connexions WebSocket et gRPC, il s'agit du nombre total d'octets envoyés du serveur au client via la connexion.

5. **`c-ip`**

   Adresse IP de la visionneuse qui a émis la demande, par exemple, `192.0.2.183` ou `2001:0db8:85a3::8a2e:0370:7334`. Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur de ce champ est l'adresse IP du proxy ou de l'équilibreur de charge. Voir aussi le champ `x-forwarded-for`.

6. **`cs-method`**

   Méthode de demande HTTP reçue de l'utilisateur.

7. **`cs(Host)`**

   Le nom de domaine de la CloudFront distribution (par exemple, d111111abcdef8.cloudfront.net).

8. **`cs-uri-stem`**

   Partie de l'URL de la requête qui identifie le chemin d'accès et l'objet (par exemple, `/images/cat.jpg`). Les points d'interrogation (?) des URL et des chaînes de requête ne sont pas inclus dans le journal.

9. **`sc-status`**

   Contient une des valeurs suivantes :

   - Code de statut HTTP de la réponse du serveur (par exemple, `200`).
   - `000`, ce qui indique que l'utilisateur a fermé la connexion avant que le serveur puisse répondre à la demande. Si l'utilisateur ferme la connexion après que le serveur a commencé à envoyer la réponse, ce champ contient le code de statut HTTP de la réponse que le serveur a commencé à envoyer.

10. **`cs(Referer)`**

    Valeur de l'en-tête `Referer` dans la demande. Nom du domaine à l'origine de la demande. Les référents courants incluent des moteurs de recherche, d'autres sites Web contenant des liens directs vers vos objets ou encore votre propre site web.

11. **`cs(User-Agent)`**

    Valeur de l'en-tête `User-Agent` dans la demande. L'en-tête `User-Agent` identifie la source de la demande, comme le type d'appareil et le navigateur ayant envoyé la demande et, si la demande provenait d'un moteur de recherche, le moteur utilisé.

12. **`cs-uri-query`**

    Partie de la chaîne de requête de l'URL de la demande, le cas échéant.

    Quand un URL ne contient pas de chaîne de requête, la valeur de ce champ est un trait d'union (-). Pour plus d'informations, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête.

13. **`cs(Cookie)`**

    En-tête `Cookie` de la demande, y compris les paires nom-valeur et les attributs associés.

    Si vous activez l'enregistrement des cookies, CloudFront enregistre les cookies dans toutes les demandes, quels que soient les cookies que vous choisissez de transmettre à l'origine. Quand une demande n'inclut pas un en-tête de cookie, la valeur de ce champ est un trait d'union (-). Pour plus d'informations sur les cookies, consultez Mise en cache de contenu basée sur des cookies.

14. **`x-edge-result-type`**

    Comment le serveur a classé la réponse après que le dernier octet a quitté le serveur. Dans certains cas, le type de résultat peut changer entre le moment où le serveur est prêt à envoyer la réponse et celui où il a fini d'envoyer celle-ci. Voir aussi le champ `x-edge-response-result-type`.

    Par exemple, dans le streaming HTTP, supposons que le serveur trouve un segment du flux dans le cache. Dans ce scénario, la valeur de ce champ est normalement `Hit`. Cependant, si l'utilisateur ferme la connexion avant que le serveur ait livré la totalité du segment, le type de résultat final (et donc la valeur de ce champ) est `Error`.

    WebSocket et les connexions gRPC auront une valeur de `Miss` pour ce champ car le contenu ne peut pas être mis en cache et est transmis directement par proxy à l'origine.

    Les valeurs possibles incluent :

    - `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.

- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'ayant pas pu être satisfaite par un objet du cache, le serveur a transmis la demande à l'origine et retourné le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.
- `CapacityExceeded` : le serveur a renvoyé un code d'erreur HTTP 503, car la capacité était insuffisante pour servir l'objet au moment de la demande.
- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`). Si la valeur du champ `sc-status` est `200`, ou si la valeur de ce champ est `Error` et que la valeur du champ `x-edge-response-result-type` est différente de `Error`, cela signifie que la demande HTTP a réussi mais que le client a été déconnecté avant de recevoir tous les octets.
- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.
- `LambdaExecutionError`— La fonction Lambda @Edge associée à la distribution n'a pas été exécutée en raison d'une association mal formée, d'un délai d'expiration de la fonction, d'un problème de AWS dépendance ou d'un autre problème général de disponibilité.

15 **`x-edge-request-id`**

Chaîne opaque qui identifie de manière unique une demande. CloudFront envoie également cette chaîne dans l'en-tête de `x-amz-cf-id` réponse.

16 **`x-host-header`**

Valeur que l'utilisateur a incluse dans l'en-tête `Host` de la demande. Si vous utilisez le nom de CloudFront domaine dans les URL de vos objets (par exemple, d111111abcdef8.cloudfront.net), ce champ contient ce nom de domaine. Si vous utilisez des noms de domaine alternatifs (CNAMES) dans vos URL d'objet (tels que www.example.com), ce champ contient l'autre nom de domaine.

Si vous utilisez des noms de domaine alternatifs, consultez `cs(Host)` dans le champ 7 pour connaître le nom de domaine associé à votre distribution.

17 **`cs-protocol`**

Protocole de la demande de l'utilisateur (`http`, `https`, `grpcs`, `ws` ou `wss`).

18. **`cs-bytes`**

    Nombre total d'octets de données que l'utilisateur a inclus dans la demande, en-têtes inclus. Pour les connexions WebSocket et gRPC, il s'agit du nombre total d'octets envoyés par le client au serveur lors de la connexion.

19. **`time-taken`**

    Nombre de secondes (au millième de seconde, par exemple 0,082) entre le moment où le serveur reçoit la demande de l'utilisateur et le moment où le serveur écrit le dernier octet de la réponse à la file d'attente de sortie, tel que mesuré sur le serveur. Du point de vue de l'utilisateur, le temps total pour obtenir la réponse complète sera plus long que cette valeur en raison de la latence réseau et de la mise en tampon TCP.

20. **`x-forwarded-for`**

    Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur du champ `c-ip` est l'adresse IP du proxy ou de l'équilibreur de charge. Dans ce cas, ce champ est l'adresse IP de l'utilisateur à l'origine de la demande. Ce champ peut contenir plusieurs adresses IP séparées par des virgules. Chaque adresse IP peut être une adresse IPv4 (par exemple, `192.0.2.183`) ou une adresse IPv6 (par exemple, `2001:0db8:85a3::8a2e:0370:7334`).

    Si l'utilisateur n'a pas utilisé de proxy HTTP ou d'équilibreur de charge, la valeur de ce champ est un trait d'union (-).

21. **`ssl-protocol`**

    Lorsque la demande utilisait le protocole HTTPS, ce champ contient le SSL/TLS protocole que l'utilisateur et le serveur ont négocié pour transmettre la demande et la réponse. Pour une liste des valeurs possibles, consultez les SSL/TLS protocoles pris en charge dansProtocoles et chiffrements pris en charge entre les spectateurs et CloudFront.

    Quand `cs-protocol` dans le champ 17 est `http`, la valeur de ce champ est un trait d'union (-).

22. **`ssl-cipher`**

    Lorsque la demande utilisait le protocole HTTPS, ce champ contient le SSL/TLS code que l'utilisateur et le serveur ont négocié pour chiffrer la demande et la réponse. Pour une liste des valeurs possibles, consultez les chiffrements pris en charge dans SSL/TLS . Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront

Quand `cs-protocol` dans le champ 17 est `http`, la valeur de ce champ est un trait d'union (-).

23 **`x-edge-response-result-type`**

Comment le serveur a classé la réponse juste avant de la retourner à l'utilisateur. Voir aussi le champ `x-edge-result-type`. Les valeurs possibles incluent :

- `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.
- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'a pas pu être satisfaite par un objet du cache, c'est pourquoi le serveur a transmis la demande au serveur d'origine et a renvoyé le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.
- `CapacityExceeded` : le serveur a renvoyé une erreur 503 car il n'avait pas suffisamment de capacité au moment de la demande pour servir l'objet.
- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`).

  Si la valeur du champ `x-edge-result-type` est `Error` et que la valeur de ce champ n'est pas `Error`, le client s'est déconnecté avant d'avoir fini le téléchargement.
- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.
- `LambdaExecutionError`— La fonction Lambda @Edge associée à la distribution n'a pas été exécutée en raison d'une association mal formée, d'un délai d'expiration de la fonction, d'un problème de AWS dépendance ou d'un autre problème général de disponibilité.

24 **`cs-protocol-version`**

Version de HTTP que l'utilisateur a spécifiée dans la requête. Les valeurs possibles incluent `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` et `HTTP/3.0`.

25 **`fle-status`**

Lorsque le chiffrement au niveau du champ est configuré pour une distribution, ce champ contient un code indiquant si le corps de la demande a bien été traité. Quand le serveur traite le corps de la demande, chiffre les valeurs dans les champs spécifiés et transfère la demande à l'origine

correctement, la valeur de ce champ est `Processed`. La valeur `x-edge-result-type` peut toujours indiquer une erreur côté client ou côté serveur dans ce cas.

Les valeurs possibles pour ce champ sont les suivantes :

- `ForwardedByContentType` – Le serveur a réacheminé la demande à l'origine sans analyse ou chiffrement, car aucun type de contenu n'était configuré.
- `ForwardedByQueryArgs` : le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car la demande contient un argument de requête qui n'était pas dans la configuration du chiffrement au niveau du champ.
- `ForwardedDueToNoProfile` – Le serveur a réacheminé la demande à l'origine sans analyse ou chiffrement, car aucun profil n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `MalformedContentTypeClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format de la valeur de l'en-tête `Content-Type` n'était pas valide.
- `MalformedInputClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format du corps de la requête n'était pas valide.
- `MalformedQueryArgsClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car un argument de requête était vide ou son format n'était pas valide.
- `RejectedByContentType` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun type de contenu n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `RejectedByQueryArgs` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun argument de requête n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `ServerError` – Le serveur d'origine a renvoyé une erreur.

Si la demande dépasse un quota de chiffrement au niveau du champ (précédemment appelé limite), ce champ contient l'un des codes d'erreur suivants, et le serveur renvoie le code d'état HTTP 400 à l'utilisateur. Pour obtenir une liste des quotas actuels de chiffrement au niveau du champ, consultez Quotas sur le chiffrement au niveau du champ.

- `FieldLengthLimitClientError` – Un champ configuré pour être chiffré a dépassé la longueur maximale autorisée.

- `FieldNumberLimitClientError` – Une demande de configuration de la distribution pour le chiffrement contient un nombre de champs supérieur à celui autorisé.
- `RequestLengthLimitClientError` – La longueur du corps de la demande dépasse la longueur maximale autorisée lorsque le chiffrement au niveau du champ est configuré.

Si le chiffrement au niveau du champ n'est pas configuré pour la distribution, la valeur de ce champ est un trait d'union (-).

26. **`fle-encrypted-fields`**

Le nombre de champs de chiffrement au niveau des champs que le serveur a chiffrés et transmis à l'origine. CloudFront les serveurs transmettent la demande traitée à l'origine pendant qu'ils chiffrent les données, de sorte que ce champ peut avoir une valeur même si la valeur de `fle-status` est une erreur.

Si le chiffrement au niveau du champ n'est pas configuré pour la distribution, la valeur de ce champ est un trait d'union (-).

27. **`c-port`**

Numéro de port de la demande depuis l'utilisateur.

28. **`time-to-first-byte`**

Nombre de secondes entre la réception de la demande et l'écriture du premier octet de la réponse, tel que mesuré sur le serveur.

29. **`x-edge-detailed-result-type`**

Ce champ contient la même valeur que le champ `x-edge-result-type`, sauf dans les cas suivants :

- Lorsque l'objet a été servi à l'utilisateur à partir de la couche Origin Shield, ce champ contient `OriginShieldHit`.
- Lorsque l'objet n'était pas dans le CloudFront cache et que la réponse était générée par une fonction Lambda @Edge de requête d'origine, ce champ contient`MissGeneratedResponse`.
- Lorsque la valeur du champ `x-edge-result-type` est `Error`, ce champ contient l'une des valeurs suivantes et présente des informations supplémentaires sur l'erreur :
  - `AbortedOrigin` – Le serveur a rencontré un problème avec l'origine.
  - `ClientCommError` – La réponse à l'utilisateur a été interrompue en raison d'un problème de communication entre le serveur et l'utilisateur.

- `ClientGeoBlocked` : la distribution est configurée de manière à refuser les demandes en provenance de l'emplacement géographique de l'utilisateur.
- `ClientHungUpRequest` – La visionneuse s'est arrêtée prématurément lors de l'envoi de la demande.
- `Error` : une erreur s'est produite pour laquelle le type d'erreur ne correspond à aucune des autres catégories. Ce type d'erreur peut se produire lorsque le serveur sert une réponse d'erreur à partir du cache.
- `InternalError`— Une CloudFront erreur interne s'est produite. Cela indique généralement que l'erreur provient de l' CloudFront infrastructure, et non de l'origine ou du visualiseur.
- `InvalidRequest` – Le serveur a reçu une demande non valide de la part de l'utilisateur.
- `InvalidRequestBlocked` – L'accès à la ressource demandée est bloqué.
- `InvalidRequestCertificate`— La distribution ne correspond pas au SSL/TLS certificat pour lequel la connexion HTTPS a été établie.
- `InvalidRequestHeader` – La demande contenait un en-tête non valide.
- `InvalidRequestMethod` – La distribution n'est pas configurée pour gérer la méthode de demande HTTP utilisée. Cela peut se produire lorsque la distribution prend en charge uniquement les demandes pouvant être mises en cache.
- `LambdaLimitExceeded`— La demande a dépassé la limite de la fonction Lambda @Edge.
- `OriginCommError` – La demande a expiré lors de la connexion à l'origine ou lors de la lecture de données à partir de l'origine.
- `OriginConnectError` : le serveur n'a pas pu se connecter à l'origine.
- `OriginContentRangeLengthError` : l'en-tête `Content-Length` de la réponse de l'origine ne correspond pas à la longueur de l'en-tête `Content-Range`.
- `OriginDnsError` : le serveur n'a pas pu résoudre le nom de domaine de l'origine.
- `OriginError` — L'origine a renvoyé une réponse incorrecte.
- `OriginHeaderTooBigError` – Un en-tête renvoyé par l'origine est trop volumineux pour être traité.
- `OriginInvalidResponseError` — L'origine a renvoyé une réponse non valide.
- `OriginReadError` : le serveur n'a pas pu lire à partir de l'origine.
- `OriginWriteError` : le serveur n'a pas pu écrire à l'origine.
- `OriginZeroSizeObjectError` — Un objet de taille zéro envoyé depuis l'origine a provoqué une erreur.

- `SlowReaderOriginError` — La visionneuse a été lente à lire le message qui a provoqué l'erreur d'origine.

30 **`sc-content-type`**

Valeur de l'en-tête `Content-Type` HTTP de la réponse.

31 **`sc-content-len`**

Valeur de l'en-tête `Content-Length` HTTP de la réponse.

32 **`sc-range-start`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de début de plage.

33 **`sc-range-end`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de fin de plage.

34 **`distribution-tenant-id`**

L'ID du locataire de distribution.

35 **`connection-id`**

Identifiant unique pour la connexion TLS.

Vous devez activer les mTLS pour vos distributions avant de pouvoir obtenir des informations pour ce champ. Pour plus d'informations, consultez Authentification TLS mutuelle avec CloudFront (Viewer MTLS).

L'exemple suivant est celui d'un fichier journal pour une distribution.

```
#Version: 1.0
#Fields: date time x-edge-location sc-bytes c-ip cs-method cs(Host) cs-uri-stem sc-
status cs(Referer) cs(User-Agent) cs-uri-query cs(Cookie) x-edge-result-type x-edge-
request-id x-host-header cs-protocol cs-bytes time-taken x-forwarded-for ssl-protocol
 ssl-cipher x-edge-response-result-type cs-protocol-version fle-status fle-encrypted-
fields c-port time-to-first-byte x-edge-detailed-result-type sc-content-type sc-
content-len sc-range-start sc-range-end
2019-12-04 21:02:31 LAX1 392 192.0.2.100 GET d111111abcdef8.cloudfront.net /
index.html 200 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;
```

```
%20x64)%20AppleWebKit/537.36%20(KHTML,%20like
%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Hit
 SOX4xwn4XV6Q4rgb7XiVGOHms_BGlTAC4KyHmureZmBNrjGdRLiNIQ== d111111abcdef8.cloudfront.net
 https 23 0.001 - TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 Hit HTTP/2.0 - - 11040 0.001 Hit
 text/html 78 - -
2019-12-04 21:02:31 LAX1 392 192.0.2.100 GET d111111abcdef8.cloudfront.net /
index.html 200 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;
%20x64)%20AppleWebKit/537.36%20(KHTML,%20like
%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Hit
 k6WGMNkEzR5BEM_SaF47gjtX9zBDO2m349OY2an0QPEaUum1ZOLrow== d111111abcdef8.cloudfront.net
 https 23 0.000 - TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 Hit HTTP/2.0 - - 11040 0.000 Hit
 text/html 78 - -
2019-12-04 21:02:31 LAX1 392 192.0.2.100 GET d111111abcdef8.cloudfront.net /
index.html 200 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;
%20x64)%20AppleWebKit/537.36%20(KHTML,%20like
%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Hit
 f37nTMVvnKvV2ZSvEsivup_c2kZ7VXzYdjC-GUQZ5qNs-89BlWazbw== d111111abcdef8.cloudfront.net
 https 23 0.001 - TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 Hit HTTP/2.0 - - 11040 0.001 Hit
 text/html 78 - -
2019-12-13 22:36:27 SEA19-C1 900 192.0.2.200 GET d111111abcdef8.cloudfront.net /
favicon.ico 502 http://www.example.com/ Mozilla/5.0%20(Windows
%20NT%2010.0;%20Win64;%20x64)%20AppleWebKit/537.36%20(KHTML,
%20like%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Error
 1pkpNfBQ39sYMnjjUQjmH2w1wdJnbHYTbag21o_3OfcQgPzdL2RSSQ== www.example.com http 675
 0.102 - - - Error HTTP/1.1 - - 25260 0.102 OriginDnsError text/html 507 - -
2019-12-13 22:36:26 SEA19-C1 900 192.0.2.200 GET d111111abcdef8.cloudfront.net / 502
 - Mozilla/5.0%20(Windows%20NT%2010.0;%20Win64;%20x64)%20AppleWebKit/537.36%20(KHTML,
%20like%20Gecko)%20Chrome/78.0.3904.108%20Safari/537.36 - - Error
 3AqrZGCnF_g0-5KOvfA7c9XLcf4YGvMFSeFdIetR1N_2y8jSis8Zxg== www.example.com http 735
 0.107 - - - Error HTTP/1.1 - - 3802 0.107 OriginDnsError text/html 507 - -
2019-12-13 22:37:02 SEA19-C2 900 192.0.2.200 GET d111111abcdef8.cloudfront.net / 502
 - curl/7.55.1 - - Error kBkDzGnceVtWHqSCqBUqtA_cEs2T3tFUBbnBNkB9El_uVRhHgcZfcw==
 www.example.com http 387 0.103 - - - Error HTTP/1.1 - - 12644 0.103 OriginDnsError
 text/html 507 - -
```

Analyse des journaux

Comme vous pouvez recevoir plusieurs journaux d'accès par heure, nous vous recommandons de combiner tous les fichiers journaux que vous avez reçus pour une période donnée en un seul fichier. Vous pouvez alors analyser les données de cette période plus précisément et plus complètement.

Pour analyser vos journaux d'accès, une solution possible consiste à utiliser Amazon Athena. Athena est un service de requêtes interactif qui peut vous aider à analyser les données relatives à des

AWS services, notamment CloudFront. Pour en savoir plus, consultez la section Interroger Amazon CloudFront Logs dans le guide de l'utilisateur d'Amazon Athena.

En outre, les articles de AWS blog suivants présentent certaines méthodes d'analyse des journaux d'accès.

- Amazon CloudFront Request Logging (pour le contenu diffusé via HTTP)
- CloudFront Journaux améliorés, désormais dotés de chaînes de requête

Utiliser des journaux d'accès en temps réel

Grâce aux journaux d'accès CloudFront en temps réel, vous pouvez obtenir des informations sur les demandes adressées à une distribution en temps réel (les journaux sont livrés quelques secondes après réception des demandes). Vous pouvez utiliser les journaux d'accès en temps réel pour surveiller, analyser et prendre des mesures en fonction des performances de diffusion du contenu.

CloudFront les journaux d'accès en temps réel sont configurables. Vous pouvez choisir :

- Le taux d'échantillonnage de vos journaux en temps réel, c'est-à-dire le pourcentage de demandes pour lesquelles vous souhaitez recevoir des enregistrements de journaux d'accès en temps réel.
- Champs spécifiques que vous souhaitez recevoir dans les enregistrements de journal.
- Comportements de cache spécifiques (modèles de chemin) pour lesquels vous souhaitez recevoir des journaux en temps réel.

CloudFront les journaux d'accès en temps réel sont transmis au flux de données de votre choix dans Amazon Kinesis Data Streams. Vous pouvez créer votre propre consommateur de flux de données Kinesis ou utiliser Amazon Data Firehose pour envoyer les données de journal à Amazon Simple Storage Service (Amazon S3), Amazon Redshift, OpenSearch Amazon Service OpenSearch (Service) ou à un service de traitement des journaux tiers.

CloudFront des frais pour les journaux d'accès en temps réel, en plus des frais que vous devez payer pour utiliser Kinesis Data Streams. Pour plus d'informations sur les tarifs, consultez les rubriques Amazon CloudFront Pricing et Amazon Kinesis Data Streams.

> **Important**
>
> Nous vous recommandons d'utiliser les journaux pour comprendre la nature des demandes concernant votre contenu, et non comme un compte rendu complet de toutes les demandes.

CloudFront fournit des journaux d'accès en temps réel dans les meilleures conditions. L'entrée du journal pour une demande particulière peut être fournie bien après le traitement réel de la demande et, dans de rares cas, une entrée du journal peut ne pas être fournie du tout. Lorsqu'une entrée de journal est omise dans les journaux d'accès en temps réel, le nombre d'entrées dans les journaux d'accès en temps réel ne correspond pas à l'utilisation indiquée dans les rapports AWS de facturation et d'utilisation.

Rubriques

- Création et utilisation de configurations de journaux d'accès en temps réel
- Comprendre les configurations des journaux d'accès en temps réel
- Création d'un consommateur Kinesis Data Streams
- Résolution des problèmes liés aux journaux d'accès en temps réel

Création et utilisation de configurations de journaux d'accès en temps réel

Pour obtenir des informations sur les demandes adressées à une distribution en temps réel, vous pouvez utiliser les configurations d'un journal d'accès en temps réel. Les journaux sont livrés dans les secondes qui suivent la réception des demandes. Vous pouvez créer une configuration de journal d'accès en temps réel dans la CloudFront console, avec le AWS Command Line Interface (AWS CLI) ou avec l' CloudFront API.

Pour utiliser une configuration de journal d'accès en temps réel, vous devez l'associer à un ou plusieurs comportements de cache dans une CloudFront distribution.

Console

Pour créer une configuration de journal d'accès en temps réel

1. Connectez-vous à la page Logs Console de gestion AWS et ouvrez-la dans la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home?#/logs.
2. Choisissez l'onglet Real-time Configurations.
3. Choisissez Créer une configuration.
4. Pour Nom, entrez un nom pour la configuration.
5. Pour Taux d'échantillonnage, entrez le pourcentage de demandes pour lesquelles vous souhaitez recevoir des journaux.

6. Pour les champs, choisissez les champs à recevoir dans les journaux d'accès en temps réel.
   - Pour inclure tous les champs CMCD dans vos journaux, choisissez CMCD all keys.
7. Pour Endpoint, choisissez un ou plusieurs flux de données Kinesis pour recevoir des journaux d'accès en temps réel.

> **Note**
>
> CloudFront les journaux d'accès en temps réel sont transmis au flux de données que vous spécifiez dans Kinesis Data Streams. Pour lire et analyser vos journaux d'accès en temps réel, vous pouvez créer votre propre consommateur de flux de données Kinesis. Vous pouvez également utiliser Firehose pour envoyer les données du journal à Amazon S3, Amazon Redshift, Amazon Service ou à un service de traitement des journaux tiers. OpenSearch

8. Dans le champ Rôle IAM, sélectionnez Créer un nouveau rôle de service ou choisissez un rôle existant. Vous devez être autorisé à créer des rôles IAM.
9. (Facultatif) Pour Distribution, choisissez un comportement de CloudFront distribution et de cache à associer à la configuration du journal d'accès en temps réel.
10. Choisissez Créer une configuration.

En cas de succès, la console affiche les détails de la configuration du journal d'accès en temps réel que vous venez de créer.

Pour plus d’informations, consultez Comprendre les configurations des journaux d'accès en temps réel.

AWS CLI

Pour créer une configuration de journal d'accès en temps réel avec le AWS CLI, utilisez la aws cloudfront create-realtime-log-config commande. Vous pouvez utiliser un fichier d’entrée pour fournir les paramètres d’entrée de la commande, plutôt que de spécifier chaque paramètre individuel comme entrée de ligne de commande.

Pour créer une configuration de journal d'accès en temps réel (CLI avec fichier d'entrée)

1. Utilisez la commande suivante pour créer un fichier nommé `rtl-config.yaml` qui contient tous les paramètres d’entrée de la commande create-realtime-log-config.

```
aws cloudfront create-realtime-log-config --generate-cli-skeleton yaml-input >
 rtl-config.yaml
```

2. Ouvrez le fichier nommé `rtl-config.yaml` que vous venez de créer. Modifiez le fichier pour spécifier les paramètres de configuration du journal d'accès en temps réel que vous souhaitez, puis enregistrez le fichier. Notez ce qui suit :

   - Pour `StreamType`, la seule valeur valide est `Kinesis`.

   Pour plus d'informations sur les paramètres de configuration longue durée en temps réel, consultez Comprendre les configurations des journaux d'accès en temps réel.

3. Utilisez la commande suivante pour créer la configuration du journal d'accès en temps réel à l'aide des paramètres d'entrée du `rtl-config.yaml` fichier.

```
aws cloudfront create-realtime-log-config --cli-input-yaml file://rtl-
config.yaml
```

En cas de succès, le résultat de la commande affiche les détails de la configuration du journal d'accès en temps réel que vous venez de créer.

Pour associer une configuration de journal d'accès en temps réel à une distribution existante (CLI avec fichier d'entrée)

1. Utilisez la commande suivante pour enregistrer la configuration de distribution pour la CloudFront distribution que vous souhaitez mettre à jour. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront get-distribution-config --id distribution_ID --output yaml >
 dist-config.yaml
```

2. Ouvrez le fichier nommé `dist-config.yaml` que vous venez de créer. Modifiez le fichier en apportant les modifications suivantes à chaque comportement de cache que vous mettez à jour afin d'utiliser une configuration de journal d'accès en temps réel.

- Dans le comportement du cache, ajoutez un champ nommé `RealtimeLogConfigArn`. Pour la valeur du champ, utilisez l'ARN de la configuration du journal d'accès en temps réel que vous souhaitez associer à ce comportement de cache.
- Renommez le champ `ETag` en `IfMatch`, mais ne modifiez pas la valeur du champ.

Enregistrez le fichier lorsque vous avez terminé.

3. Utilisez la commande suivante pour mettre à jour la distribution afin d'utiliser la configuration du journal d'accès en temps réel. Remplacez *`distribution_ID`* par l'ID de la distribution.

```
aws cloudfront update-distribution --id distribution_ID --cli-input-yaml file://
dist-config.yaml
```

En cas de réussite, la sortie de la commande affiche les détails de la distribution que vous venez de mettre à jour.

API

Pour créer une configuration de journal d'accès en temps réel avec l' CloudFront API, utilisez l'opération CreateRealtimeLogConfigAPI. Pour plus d'informations sur les paramètres que vous spécifiez dans cet appel d'API, consultez Comprendre les configurations des journaux d'accès en temps réel la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Après avoir créé une configuration de journal d'accès en temps réel, vous pouvez l'associer à un comportement de cache en utilisant l'une des opérations d'API suivantes :

- Pour l'associer à un comportement de cache dans une distribution existante, utilisez UpdateDistribution.
- Pour l'associer à un comportement de cache dans une nouvelle distribution, utilisez CreateDistribution.

Pour ces deux opérations d'API, fournissez l'ARN de la configuration du journal d'accès en temps réel `RealtimeLogConfigArn` sur le terrain, dans un comportement de cache. Pour plus d'informations sur les autres champs que vous spécifiez dans ces appels d'API, consultez Référence de tous les paramètres de distribution la documentation de référence de l'API pour votre AWS SDK ou autre client d'API.

Comprendre les configurations des journaux d'accès en temps réel

Pour utiliser les journaux d'accès CloudFront en temps réel, vous devez commencer par créer une configuration de journal d'accès en temps réel. La configuration du journal d'accès en temps réel contient des informations sur les champs de journal que vous souhaitez recevoir, le taux d'échantillonnage des enregistrements de journal et le flux de données Kinesis dans lequel vous souhaitez transmettre les journaux.

Plus précisément, une configuration de journal d'accès en temps réel contient les paramètres suivants :

Table des matières

- Nom
- Taux d’échantillonnage
- Champs
- Point de terminaison (Kinesis Data Streams)
- Rôle IAM

Nom

Nom permettant d'identifier la configuration du journal d'accès en temps réel.

Taux d’échantillonnage

Le taux d’échantillonnage est un nombre entier compris entre 1 et 100 (inclus) qui détermine le pourcentage de demandes utilisateur envoyées à Kinesis Data Streams sous forme d’enregistrements de journal d’accès en temps réel. Pour inclure chaque demande utilisateur dans vos journaux d’accès en temps réel, spécifiez 100 pour le taux d’échantillonnage. Vous pouvez choisir un taux d’échantillonnage inférieur pour réduire les coûts tout en recevant un échantillon représentatif des données de demande dans vos journaux d’accès en temps réel.

Champs

Liste des champs inclus dans chaque enregistrement du journal d'accès en temps réel. Chaque enregistrement de journal peut contenir jusqu’à 40 champs ; vous pouvez choisir de recevoir tous les champs disponibles ou uniquement les champs dont vous avez besoin pour surveiller et analyser les performances.

La liste suivante contient chaque nom de champ et une description des informations contenues dans ce champ. Les champs sont répertoriés dans l'ordre dans lequel ils apparaissent dans les enregistrements de journal qui sont distribués à Kinesis Data Streams.

Les champs 46 à 63 correspondent aux données client média communes (CMCD) que les lecteurs multimédias peuvent envoyer aux CDN avec chaque demande. Vous pouvez utiliser ces données pour comprendre chaque demande, notamment le type de média (audio, vidéo), le taux de lecture et la durée de diffusion. Ces champs n'apparaîtront dans vos journaux d'accès en temps réel que s'ils sont envoyés à CloudFront.

1. **`timestamp`**

   Date et heure auxquelles le serveur Edge a fini de répondre à la demande.

2. **`c-ip`**

   Adresse IP de la visionneuse qui a émis la demande, par exemple, `192.0.2.183` ou `2001:0db8:85a3::8a2e:0370:7334`. Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur de ce champ est l'adresse IP du proxy ou de l'équilibreur de charge. Voir aussi le champ `x-forwarded-for`.

3. **`s-ip`**

   L'adresse IP du CloudFront serveur qui a répondu à la demande, par exemple, `192.0.2.183` ou`2001:0db8:85a3::8a2e:0370:7334`.

4. **`time-to-first-byte`**

   Nombre de secondes entre la réception de la demande et l'écriture du premier octet de la réponse, tel que mesuré sur le serveur.

5. **`sc-status`**

   Code de statut HTTP de la réponse du serveur (par exemple, `200`).

6. **`sc-bytes`**

   Nombre total d'octets envoyés par le serveur à l'utilisateur en réponse à la demande, en-têtes inclus. Pour les connexions gRPC WebSocket et gRPC, il s'agit du nombre total d'octets envoyés par le serveur au client via la connexion.

7. **`cs-method`**

   Méthode de demande HTTP reçue de l'utilisateur.

8. **`cs-protocol`**

   Protocole de la demande de l'utilisateur (`http`, `https`, `grpcs`, `ws` ou `wss`).

9. **`cs-host`**

   Valeur que l'utilisateur a incluse dans l'en-tête `Host` de la demande. Si vous utilisez le nom de CloudFront domaine dans les URL de vos objets (par exemple d111111abcdef8.cloudfront.net), ce champ contient ce nom de domaine. Si vous utilisez des noms de domaine alternatifs (CNAMES) dans vos URL d'objet (tels que www.example.com), ce champ contient l'autre nom de domaine.

10. **`cs-uri-stem`**

    L'URL entière de la demande, y compris la chaîne de requête (le cas échéant), mais sans le nom de domaine. Par exemple : `/images/cat.jpg?mobile=true`.

    > **Note**
    >
    > Dans les journaux standard, la valeur `cs-uri-stem` n'inclut pas la chaîne de requête.

11. **`cs-bytes`**

    Nombre total d'octets de données que l'utilisateur a inclus dans la demande, en-têtes inclus. Pour les connexions gRPC WebSocket et gRPC, il s'agit du nombre total d'octets envoyés par le client au serveur lors de la connexion.

12. **`x-edge-location`**

    Emplacement périphérique ayant servi la demande. Chaque emplacement périphérique est identifié par un code à trois lettres et un numéro attribué arbitrairement (par exemple, DFW3). Le code à trois lettres correspond généralement au code IATA (International Air Transport Association) d'un aéroport proche de l'emplacement périphérique. (Ces abréviations peuvent changer à l'avenir.)

13. **`x-edge-request-id`**

    Chaîne opaque qui identifie une demande de manière unique. CloudFront envoie également cette chaîne dans l'en-tête de `x-amz-cf-id` réponse.

14. **`x-host-header`**

    Le nom de domaine de la CloudFront distribution (par exemple, d111111abcdef8.cloudfront.net).

15. **`time-taken`**

Nombre de secondes (au millième de seconde, par exemple 0,082) entre le moment où le serveur reçoit la demande de l'utilisateur et le moment où le serveur écrit le dernier octet de la réponse à la file d'attente de sortie, tel que mesuré sur le serveur. Du point de vue de l'utilisateur, le temps total pour obtenir la réponse complète sera plus long que cette valeur en raison de la latence réseau et de la mise en tampon TCP.

16. **`cs-protocol-version`**

    Version de HTTP que l'utilisateur a spécifiée dans la requête. Les valeurs possibles incluent `HTTP/0.9`, `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0` et `HTTP/3.0`.

17. **`c-ip-version`**

    Version IP de la demande (IPv4 ou IPv6).

18. **`cs-user-agent`**

    Valeur de l'en-tête `User-Agent` dans la demande. L'en-tête `User-Agent` identifie la source de la demande, comme le type d'appareil et le navigateur ayant envoyé la demande et, si la demande provenait d'un moteur de recherche, le moteur utilisé.

19. **`cs-referer`**

    Valeur de l'en-tête `Referer` dans la demande. Nom du domaine à l'origine de la demande. Les référents courants incluent des moteurs de recherche, d'autres sites Web contenant des liens directs vers vos objets ou encore votre propre site web.

20. **`cs-cookie`**

    En-tête `Cookie` de la demande, y compris les paires nom-valeur et les attributs associés.

    > **Note**
    >
    > Ce champ est tronqué à 800 octets.

21. **`cs-uri-query`**

    Partie de la chaîne de requête de l'URL de la demande, le cas échéant.

22. **`x-edge-response-result-type`**

    Comment le serveur a classé la réponse juste avant de la retourner à l'utilisateur. Voir aussi le champ `x-edge-result-type`. Les valeurs possibles incluent :

- `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.
- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'a pas pu être satisfaite par un objet du cache, c'est pourquoi le serveur a transmis la demande au serveur d'origine et a renvoyé le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.
- `CapacityExceeded` : le serveur a renvoyé une erreur 503 car il n'avait pas suffisamment de capacité au moment de la demande pour servir l'objet.
- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`).

  Si la valeur du champ `x-edge-result-type` est `Error` et que la valeur de ce champ n'est pas `Error`, le client s'est déconnecté avant d'avoir fini le téléchargement.
- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.
- `LambdaExecutionError`— La fonction Lambda @Edge associée à la distribution ne s'est pas terminée en raison d'une association mal formée, d'un délai d'expiration de la fonction, d'un problème de AWS dépendance ou d'un autre problème de disponibilité générale.

23**`x-forwarded-for`**

Si l'utilisateur a utilisé un proxy HTTP ou un équilibreur de charge pour envoyer la demande, la valeur du champ `c-ip` est l'adresse IP du proxy ou de l'équilibreur de charge. Dans ce cas, ce champ est l'adresse IP de l'utilisateur à l'origine de la demande. Ce champ peut contenir plusieurs adresses IP séparées par des virgules. Chaque adresse IP peut être une adresse IPv4 (par exemple, `192.0.2.183`) ou une adresse IPv6 (par exemple, `2001:0db8:85a3::8a2e:0370:7334`).

24**`ssl-protocol`**

Lorsque la demande a utilisé le protocole HTTPS, ce champ contient le SSL/TLS protocole négocié par le spectateur et le serveur pour transmettre la demande et la réponse. Pour obtenir la liste des valeurs possibles, consultez les SSL/TLS protocoles pris en charge dansProtocoles et chiffrements pris en charge entre les spectateurs et CloudFront.

25**`ssl-cipher`**

Lorsque la demande a utilisé le protocole HTTPS, ce champ contient le SSL/TLS code que le lecteur et le serveur ont négocié pour chiffrer la demande et la réponse. Pour une liste des valeurs possibles, consultez les chiffrements pris en charge dans SSL/TLS . Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront

26 **`x-edge-result-type`**

Comment le serveur a classé la réponse après que le dernier octet a quitté le serveur. Dans certains cas, le type de résultat peut changer entre le moment où le serveur est prêt à envoyer la réponse et celui où il a fini d'envoyer celle-ci. Voir aussi le champ `x-edge-response-result-type`.

Par exemple, dans le streaming HTTP, supposons que le serveur trouve un segment du flux dans le cache. Dans ce scénario, la valeur de ce champ est normalement `Hit`. Cependant, si l'utilisateur ferme la connexion avant que le serveur ait livré la totalité du segment, le type de résultat final (et donc la valeur de ce champ) est `Error`.

WebSocket et les connexions gRPC auront une valeur égale à `Miss` pour ce champ car le contenu ne peut pas être mis en cache et est transmis directement à l'origine par proxy.

Les valeurs possibles incluent :

- `Hit` – Le serveur a servi l'objet à l'utilisateur depuis le cache.
- `RefreshHit` – Le serveur a trouvé l'objet dans le cache, mais l'objet avait expiré. Le serveur a donc contacté l'origine pour vérifier que le cache possédait la dernière version de l'objet.
- `Miss` – La demande n'ayant pas pu être satisfaite par un objet du cache, le serveur a transmis la demande à l'origine et retourné le résultat à l'utilisateur.
- `LimitExceeded`— La demande a été refusée car un CloudFront quota (anciennement appelé limite) a été dépassé.
- `CapacityExceeded` : le serveur a renvoyé un code d'erreur HTTP 503, car la capacité était insuffisante pour servir l'objet au moment de la demande.
- `Error` – Généralement, cela signifie que la demande a entraîné une erreur client (la valeur du champ `sc-status` est dans la plage `4xx`) ou une erreur serveur (la valeur du champ `sc-status` est dans la plage `5xx`). Si la valeur du champ `sc-status` est `200`, ou si la valeur de ce champ est `Error` et que la valeur du champ `x-edge-response-result-type` est différente de `Error`, cela signifie que la demande HTTP a réussi mais que le client a été déconnecté avant de recevoir tous les octets.

- `Redirect` – Le serveur a redirigé l'utilisateur depuis HTTP vers HTTPS en fonction des paramètres de distribution.
- `LambdaExecutionError`— La fonction Lambda @Edge associée à la distribution ne s'est pas terminée en raison d'une association mal formée, d'un délai d'expiration de la fonction, d'un problème de AWS dépendance ou d'un autre problème de disponibilité générale.

27. **`fle-encrypted-fields`**

    Le nombre de champs de chiffrement au niveau des champs que le serveur a chiffrés et transmis à l'origine. CloudFront les serveurs transmettent la demande traitée à l'origine au fur et à mesure qu'ils chiffrent les données. Ce champ peut donc avoir une valeur même si la valeur de `fle-status` est une erreur.

28. **`fle-status`**

    Lorsque le chiffrement au niveau du champ est configuré pour une distribution, ce champ contient un code indiquant si le corps de la demande a bien été traité. Quand le serveur traite le corps de la demande, chiffre les valeurs dans les champs spécifiés et transfère la demande à l'origine correctement, la valeur de ce champ est `Processed`. La valeur `x-edge-result-type` peut toujours indiquer une erreur côté client ou côté serveur dans ce cas.

    Les valeurs possibles pour ce champ sont les suivantes :

    - `ForwardedByContentType` – Le serveur a réacheminé la demande à l'origine sans analyse ou chiffrement, car aucun type de contenu n'était configuré.
    - `ForwardedByQueryArgs` : le serveur a réacheminé la demande vers l'origine sans analyse ou chiffrement, car la demande contient un argument de requête qui n'était pas dans la configuration du chiffrement au niveau du champ.
    - `ForwardedDueToNoProfile` – Le serveur a réacheminé la demande à l'origine sans analyse ou chiffrement, car aucun profil n'était spécifié dans la configuration du chiffrement au niveau du champ.
    - `MalformedContentTypeClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format de la valeur de l'en-tête `Content-Type` n'était pas valide.
    - `MalformedInputClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car le format du corps de la requête n'était pas valide.

- `MalformedQueryArgsClientError` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car un argument de requête était vide ou son format n'était pas valide.
- `RejectedByContentType` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun type de contenu n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `RejectedByQueryArgs` – Le serveur a rejeté la demande et a renvoyé le code de statut HTTP 400 à l'utilisateur, car aucun argument de requête n'était spécifié dans la configuration du chiffrement au niveau du champ.
- `ServerError` – Le serveur d'origine a renvoyé une erreur.

Si la demande dépasse un quota de chiffrement au niveau du champ (précédemment appelé limite), ce champ contient l'un des codes d'erreur suivants, et le serveur renvoie le code d'état HTTP 400 à l'utilisateur. Pour obtenir une liste des quotas actuels de chiffrement au niveau du champ, consultez Quotas sur le chiffrement au niveau du champ.

- `FieldLengthLimitClientError` – Un champ configuré pour être chiffré a dépassé la longueur maximale autorisée.
- `FieldNumberLimitClientError` – Une demande de configuration de la distribution pour le chiffrement contient un nombre de champs supérieur à celui autorisé.
- `RequestLengthLimitClientError` – La longueur du corps de la demande dépasse la longueur maximale autorisée lorsque le chiffrement au niveau du champ est configuré.

29 **`sc-content-type`**

Valeur de l'en-tête `Content-Type` HTTP de la réponse.

30 **`sc-content-len`**

Valeur de l'en-tête `Content-Length` HTTP de la réponse.

31 **`sc-range-start`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de début de plage.

32 **`sc-range-end`**

Lorsque la réponse contient l'en-tête `Content-Range` HTTP, ce champ contient la valeur de fin de plage.

33 **`c-port`**

Numéro de port de la demande depuis l'utilisateur.

34 **`x-edge-detailed-result-type`**

Ce champ contient la même valeur que le champ `x-edge-result-type`, sauf dans les cas suivants :

- Lorsque l'objet a été servi à l'utilisateur à partir de la couche Origin Shield, ce champ contient `OriginShieldHit`.
- Lorsque l'objet n'était pas dans le CloudFront cache et que la réponse a été générée par une fonction Lambda @Edge de demande d'origine, ce champ contient. `MissGeneratedResponse`
- Lorsque la valeur du champ `x-edge-result-type` est `Error`, ce champ contient l'une des valeurs suivantes et présente des informations supplémentaires sur l'erreur :
  - `AbortedOrigin` – Le serveur a rencontré un problème avec l'origine.
  - `ClientCommError` – La réponse à l'utilisateur a été interrompue en raison d'un problème de communication entre le serveur et l'utilisateur.
  - `ClientGeoBlocked` : la distribution est configurée de manière à refuser les demandes en provenance de l'emplacement géographique de l'utilisateur.
  - `ClientHungUpRequest` – La visionneuse s'est arrêtée prématurément lors de l'envoi de la demande.
  - `Error` : une erreur s'est produite pour laquelle le type d'erreur ne correspond à aucune des autres catégories. Ce type d'erreur peut se produire lorsque le serveur sert une réponse d'erreur à partir du cache.
  - `InternalError`— Une CloudFront erreur interne s'est produite. Cela indique généralement que l'erreur provient de l' CloudFront infrastructure, et non de l'origine ou du lecteur.
  - `InvalidRequest` – Le serveur a reçu une demande non valide de la part de l'utilisateur.
  - `InvalidRequestBlocked` – L'accès à la ressource demandée est bloqué.
  - `InvalidRequestCertificate`— La distribution ne correspond pas au SSL/TLS certificat pour lequel la connexion HTTPS a été établie.
  - `InvalidRequestHeader` – La demande contenait un en-tête non valide.
  - `InvalidRequestMethod` – La distribution n'est pas configurée pour gérer la méthode de demande HTTP utilisée. Cela peut se produire lorsque la distribution prend en charge uniquement les demandes pouvant être mises en cache.
  - `LambdaLimitExceeded`— La demande a dépassé la limite de fonction Lambda @Edge.

- `OriginCommError` – La demande a expiré lors de la connexion à l'origine ou lors de la lecture de données à partir de l'origine.
- `OriginConnectError` : le serveur n'a pas pu se connecter à l'origine.
- `OriginContentRangeLengthError` : l'en-tête `Content-Length` de la réponse de l'origine ne correspond pas à la longueur de l'en-tête `Content-Range`.
- `OriginDnsError` : le serveur n'a pas pu résoudre le nom de domaine de l'origine.
- `OriginError` — L'origine a renvoyé une réponse incorrecte.
- `OriginHeaderTooBigError` – Un en-tête renvoyé par l'origine est trop volumineux pour être traité.
- `OriginInvalidResponseError` — L'origine a renvoyé une réponse non valide.
- `OriginReadError` : le serveur n'a pas pu lire à partir de l'origine.
- `OriginWriteError` : le serveur n'a pas pu écrire à l'origine.
- `OriginZeroSizeObjectError` — Un objet de taille zéro envoyé depuis l'origine a provoqué une erreur.
- `SlowReaderOriginError` — La visionneuse a été lente à lire le message qui a provoqué l'erreur d'origine.

35 **`c-country`**

Code de pays qui représente l'emplacement géographique de l'utilisateur, déterminé par l'adresse IP de l'utilisateur. Pour obtenir une liste des codes de pays, consultez ISO 3166-1 alpha-2.

36 **`cs-accept-encoding`**

Valeur de l'en-tête `Accept-Encoding` dans la demande de l'utilisateur.

37 **`cs-accept`**

Valeur de l'en-tête `Accept` dans la demande de l'utilisateur.

38 **`cache-behavior-path-pattern`**

Modèle de chemin qui identifie le comportement du cache correspondant à la demande de l'utilisateur.

39 **`cs-headers`**

En-têtes HTTP (noms et valeurs) dans la demande de l'utilisateur.

> **Note**
>
> Ce champ est tronqué à 800 octets.

40. **`cs-header-names`**

    Noms des en-têtes HTTP (et non des valeurs) dans la demande de l'utilisateur.

    > **Note**
    >
    > Ce champ est tronqué à 800 octets.

41. **`cs-headers-count`**

    Nombre d'en-têtes HTTP dans la demande de l'utilisateur.

42. **`primary-distribution-id`**

    Lorsque le déploiement continu est activé, cet ID identifie la distribution principale dans la distribution actuelle.

43. **`primary-distribution-dns-name`**

    Lorsque le déploiement continu est activé, cette valeur indique le nom de domaine principal associé à la CloudFront distribution actuelle (par exemple, d111111abcdef8.cloudfront.net).

44. **`origin-fbl`**

    Le nombre de secondes de latence du premier octet entre CloudFront et votre origine.

45. **`origin-lbl`**

    Le nombre de secondes de latence du dernier octet entre CloudFront et votre origine.

46. **`asn`**

    Numéro de système autonome (ASN) de l'utilisateur.

47.

    > **Champs CMCD dans les journaux d'accès en temps réel**
    >
    > Pour plus d'informations sur ces champs, consultez le CTA-5004 document CTA Specification Web Application Video Ecosystem - Common Media Client Data.

48. **`cmcd-encoded-bitrate`**

    Le débit binaire encodé de l'objet audio ou vidéo demandé.

49. **`cmcd-buffer-length`**

    La longueur du tampon de l'objet média demandé.

50. **`cmcd-buffer-starvation`**

    Indique si le tampon s'est retrouvé à court de données entre la demande précédente et la demande de l'objet. Cela peut entraîner le lecteur dans un état de rebuffering, ce qui peut bloquer la lecture vidéo ou audio.

51. **`cmcd-content-id`**

    Une chaîne unique qui identifie le contenu actuel.

52. **`cmcd-object-duration`**

    La durée de lecture de l'objet demandé (en millisecondes).

53. **`cmcd-deadline`**

    Le délai à compter de la demande dans lequel le premier échantillon de cet objet doit être disponible, afin d'éviter tout état de sous-alimentation du tampon ou tout autre problème de lecture.

54. **`cmcd-measured-throughput`**

    Le débit entre le client et le serveur, tel que mesuré par le client.

55. **`cmcd-next-object-request`**

    Le chemin d'accès relatif du prochain objet demandé.

56. **`cmcd-next-range-request`**

    Si la demande suivante est une demande d'objet partielle, cette chaîne indique la plage d'octets à demander.

57. **`cmcd-object-type`**

    Le type de média de l'objet actuellement demandé.

58. **`cmcd-playback-rate`**

1 pour une lecture en temps réel, 2 pour une lecture à double vitesse, 0 lorsque la lecture est arrêtée.

59. **`cmcd-requested-maximum-throughput`**

    Le débit maximal demandé que le client considère comme suffisant pour la livraison des ressources.

60. **`cmcd-streaming-format`**

    Le format de streaming qui définit la demande en cours.

61. **`cmcd-session-id`**

    Un GUID identifiant la session de lecture en cours.

62. **`cmcd-stream-type`**

    Jeton identifiant la disponibilité du segment. `v` = tous les segments sont disponibles. `l` = les segments deviennent disponibles au fil du temps.

63. **`cmcd-startup`**

    La clé est incluse sans valeur si l'objet est requis de toute urgence lors du démarrage, d'une opération de recherche, ou lors de la récupération après un événement de tampon vide.

64. **`cmcd-top-bitrate`**

    La version au débit binaire le plus élevé que le client peut lire.

65. **`cmcd-version`**

    La version de cette spécification utilisée pour interpréter les noms de clés et les valeurs définis. Si cette clé est omise, le client et le serveur doivent interpréter les valeurs telles qu'elles sont définies par la version 1.

66. **`r-host`**

    Ce champ est envoyé pour les demandes d'origine et indique le domaine du serveur d'origine utilisé pour servir l'objet. En cas d'erreur, vous pouvez utiliser ce champ pour trouver la dernière origine tentée, par exemple : *`cd8jhdejh6a`*`.mediapackagev2.us-east-1.amazonaws.com`.

67. **`sr-reason`**

    Ce champ indique la raison pour laquelle l'origine a été sélectionnée. Il est vide lorsqu'une demande adressée à l'origine principale aboutit.

Si un basculement d'origine se produit, le champ contiendra le code d'erreur HTTP ayant provoqué le basculement, comme `Failover:403` ou `Failover:502`. En cas de basculement d'origine, si la demande réessayée échoue également et que vous n'avez pas configuré de pages d'erreur personnalisées, alors `r-status` indique la réponse de la deuxième origine. Toutefois, si vous avez configuré des pages d'erreur personnalisées en plus du basculement d'origine, ce champ contiendra la réponse de la seconde origine si la demande a échoué et qu'une page d'erreur personnalisée a été renvoyée à la place.

S'il n'y a pas de basculement, mais qu'une sélection d'origine MQAR (résilience tenant compte de la qualité média) est effectuée, l'entrée sera enregistrée sous `MediaQuality`. Pour plus d'informations, consultez Résilience tenant compte de la qualité média.

68 **`x-edge-mqcs`**

Ce champ indique le Media Quality Confidence Score (MQCS) (plage : 0 à 100) pour les segments multimédias CloudFront extraits dans les en-têtes de réponse CMSD de la version v2. MediaPackage Ce champ est disponible pour les demandes correspondant à un comportement de cache ayant un groupe MQAR-enabled d'origine. CloudFront enregistre ce champ pour les segments multimédias qui sont également diffusés à partir de son cache en plus des demandes d'origine. Pour plus d'informations, consultez Résilience tenant compte de la qualité média.

69 **`distribution-tenant-id`**

L'ID du locataire de distribution.

70 **`connection-id`**

Identifiant unique pour la connexion TLS.

Vous devez activer les MTLs pour vos distributions avant de pouvoir obtenir des informations pour ce champ. Pour plus d'informations, consultez Authentification TLS mutuelle avec CloudFront (Viewer MTLS).

71 **`viewer-request-log-data`**

Données personnalisées que votre CloudFront fonction de demande d'audience envoie à l'aide de la méthode d'`cf.logCustomData()`assistance. Ce champ contient la valeur de chaîne que vous avez transmise à la méthode lors de l'événement de demande du spectateur. CloudFront URL-encodes la valeur et la tronque à un maximum de 800 octets. Si aucune CloudFront fonction n'est associée à l'événement de demande du spectateur, ou si la fonction n'appelle

pas`cf.logCustomData()`, ce champ est défini comme tel-. Pour plus d'informations, consultez Méthodes d'assistance générales.

72. **`viewer-response-log-data`**

    Données personnalisées que votre CloudFront fonction de réponse du spectateur envoie à l'aide de la méthode d'`cf.logCustomData()`assistance. Ce champ contient la valeur de chaîne que vous avez transmise à la méthode lors de l'événement de réponse du spectateur. CloudFront URL-encodes la valeur et la tronque à un maximum de 800 octets. Si aucune CloudFront fonction n'est associée à l'événement de réponse du spectateur, ou si la fonction n'appelle pas`cf.logCustomData()`, ce champ est défini comme tel-. Pour plus d'informations, consultez Méthodes d'assistance générales.

Point de terminaison (Kinesis Data Streams)

Le point de terminaison contient des informations sur le Kinesis Data Streams dans lequel vous souhaitez envoyer des journaux en temps réel. Vous fournissez Amazon Resource Name (ARN) du flux de données.

Pour plus d'informations sur la création d'un Kinesis Data Streams, consultez les rubriques suivantes du Guide de l'utilisateur Amazon Kinesis Data Streams.

- Création et gestion de flux
- Effectuez des opérations de base sur Kinesis Data Streams à l'aide du AWS CLI
- Création d'un flux (utilise le AWS SDK pour Java)

Lorsque vous créez un flux de données, vous devez spécifier le nombre de partitions. Utilisez les informations suivantes pour vous aider à estimer le nombre de partitions dont vous avez besoin.

Pour estimer le nombre de partitions pour votre flux de données Kinesis

1. Calculez (ou estimez) le nombre de demandes par seconde que votre distribution CloudFront reçoit.

   Vous pouvez utiliser les rapports CloudFront d'utilisation (dans la CloudFront console) et les CloudFront métriques (dans les CloudWatch consoles CloudFront et Amazon) pour vous aider à calculer le nombre de demandes par seconde.
2. Déterminez la taille typique d'un seul enregistrement de journal d'accès en temps réel.

En général, un seul enregistrement de journal est d'environ 500 octets. Un enregistrement volumineux qui contient tous les champs disponibles est généralement d'environ 1 Ko.

Si vous ne connaissez pas la taille de vos enregistrements, vous pouvez activer les journaux en temps réel avec un faible taux d'échantillonnage (par exemple, 1 %), puis calculer la taille moyenne des enregistrements en utilisant les données de surveillance dans Kinesis Data Streams (nombre total d'octets entrants divisé par le nombre total d'enregistrements).

3. Sur la page de tarification d'Amazon Kinesis Data Streams, Calculateur de tarification AWS sous, choisissez Create your custom estimate now.

   - Dans le calculateur, entrez le nombre de demandes (enregistrements) par seconde.
   - Entrez la taille moyenne d'un enregistrement de journal individuel.
   - Sélectionnez Afficher les calculs.

   Le calculateur de tarification vous indique le nombre de partitions nécessaire et le coût estimé.

Rôle IAM

Rôle Gestion des identités et des accès AWS (IAM) qui donne l' CloudFront autorisation de fournir des journaux d'accès en temps réel à votre flux de données Kinesis.

Lorsque vous créez une configuration de journal d'accès en temps réel avec la CloudFront console, vous pouvez choisir Créer un nouveau rôle de service pour permettre à la console de créer le rôle IAM pour vous.

Lorsque vous créez une configuration de journal d'accès en temps réel avec AWS CloudFormation l' CloudFront API (AWS CLI ou le SDK), vous devez créer vous-même le rôle IAM et fournir l'ARN du rôle. Pour créer le rôle IAM vous-même, utilisez les politiques suivantes.

Stratégie d'approbation de rôle IAM

Pour utiliser la politique de confiance des rôles IAM suivante, remplacez-la *111122223333* par votre Compte AWS numéro. L'`Condition`élément de cette politique permet d'éviter le problème de confusion des adjoints, car ils ne CloudFront peuvent assumer ce rôle qu'au nom d'une distribution de votre entreprise Compte AWS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Stratégie d'autorisations de rôle IAM pour un flux de données non chiffré

Pour appliquer la politique suivante, remplacez-la *arn:aws:kinesis:us-east-2:123456789012:stream/StreamName* par l'ARN de votre flux de données Kinesis.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
```

```
            ]
        }
    ]
}
```

Stratégie d'autorisations de rôle IAM pour un flux de données chiffré

Pour appliquer la politique suivante, remplacez-le *arn:aws:kinesis:us-east-2:123456789012:stream/StreamName* par l'ARN de votre flux de données Kinesis et *arn:aws:kms:us-east-2:123456789012:key/e58a3d0b-fe4f-4047-a495-ae03cc73d486* par l'ARN de votre. AWS KMS key

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStreamSummary",
                "kinesis:DescribeStream",
                "kinesis:PutRecord",
                "kinesis:PutRecords"
            ],
            "Resource": [
                "arn:aws:kinesis:us-east-2:123456789012:stream/StreamName"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/e58a3d0b-fe4f-4047-a495-
ae03cc73d486"
            ]
        }
    ]
}
```

Création d’un consommateur Kinesis Data Streams

Pour lire et analyser vos journaux d'accès en temps réel, vous créez ou utilisez un client Kinesis Data Streams. Lorsque vous créez un consommateur pour les journaux CloudFront en temps réel, il est important de savoir que les champs de chaque enregistrement de journal d'accès en temps réel sont toujours livrés dans le même ordre, comme indiqué dans la Champs section. Assurez-vous que vous créez votre consommateur en fonction de cet ordre fixe.

Par exemple, considérez une configuration de journal d'accès en temps réel qui inclut uniquement les trois champs suivants : `time-to-first-bytesc-status`, et`c-country`. Dans ce scénario, le dernier champ, `c-country`, est toujours le champ numéro 3 dans chaque enregistrement de journal. Toutefois, si vous ajoutez ultérieurement des champs à la configuration du journal d'accès en temps réel, le placement de chaque champ dans un enregistrement peut changer.

Par exemple, si vous ajoutez les champs `sc-bytes` et `time-taken` à la configuration du journal d'accès en temps réel, ces champs sont insérés dans chaque enregistrement du journal conformément à l'ordre indiqué dans la Champs section. L'ordre final des cinq champs est `time-to-first-byte`, `sc-status`, `sc-bytes`, `time-taken` et `c-country`. Le champ `c-country` était à l'origine le champ numéro 3, mais il est maintenant le champ numéro 5. Assurez-vous que votre application grand public peut gérer les champs qui changent de position dans un enregistrement de journal, au cas où vous ajouteriez des champs à la configuration de votre journal d'accès en temps réel.

Résolution des problèmes liés aux journaux d'accès en temps réel

Après avoir créé une configuration de journal d'accès en temps réel, vous constaterez peut-être qu'aucun enregistrement (ou pas tous les enregistrements) n'est transmis à Kinesis Data Streams. Dans ce cas, vous devez d'abord vérifier que votre distribution CloudFront reçoit des demandes de l'utilisateur. Le cas échéant, vous pouvez vérifier le paramètre suivant pour poursuivre le dépannage.

Autorisations de rôle IAM

> Pour fournir des enregistrements de journaux d'accès en temps réel à votre flux de données Kinesis, CloudFront utilisez le rôle IAM dans la configuration du journal d'accès en temps réel. Assurez-vous que la stratégie d'approbation de rôle et la stratégie d'autorisations de rôle correspondent aux stratégies indiquées dans Rôle IAM.

Limitation des Kinesis Data Streams

Si CloudFront les enregistrements du journal d'accès en temps réel sont écrits dans votre flux de données Kinesis plus rapidement que le flux ne peut le gérer, Kinesis Data Streams peut limiter le nombre de demandes provenant de. CloudFront Dans ce cas, vous pouvez augmenter le nombre de partitions dans votre flux de données Kinesis. Chaque partition peut prendre en charge des écritures jusqu'à 1 000 enregistrements par seconde, jusqu'à un maximum d'écritures de données de 1 Mo par seconde.

Journaux des fonctions de périphérie

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir les journaux de vos fonctions périphériques, à la fois Lambda @Edge et CloudFront Functions. Vous pouvez accéder aux journaux à l'aide de la CloudWatch console ou de l'API CloudWatch Logs.

> **Important**
>
> Nous vous recommandons d'utiliser les journaux pour comprendre la nature des demandes concernant votre contenu, et non comme un compte rendu complet de toutes les demandes. CloudFront fournit des journaux des fonctions de pointe dans les meilleures conditions. L'entrée du journal pour une demande particulière peut être fournie bien après le traitement réel de la demande et, dans de rares cas, une entrée du journal peut ne pas être fournie du tout. Quand une entrée de journal est omise des journaux de fonctions de périphérie, le nombre d'entrées des journaux de fonctions de périphérie ne correspond pas à l'utilisation qui apparaît dans les rapports d'utilisation et de facturation AWS .

Rubriques

- Journaux Lambda@Edge
- CloudFront Journaux de fonctions

Journaux Lambda@Edge

Lambda @Edge envoie automatiquement des journaux de fonctions à Logs, créant ainsi des flux de CloudWatch journaux dans l' Régions AWS endroit où les fonctions sont invoquées. Lorsque vous créez ou modifiez une fonction dans AWS Lambda, vous pouvez soit utiliser le nom du groupe de CloudWatch journaux par défaut, soit le personnaliser.

- Le nom du groupe de journaux par défaut est `/aws/lambda/<FunctionName>`, où *`<FunctionName>`* est le nom que vous avez indiqué lors de la création de la fonction. Lors de l'envoi de journaux à CloudWatch, Lambda @Edge ajoute automatiquement le `us-east-1` préfixe au nom de la fonction, de sorte que le nom du groupe de journaux soit. `/aws/lambda/us-east-1.`*`<FunctionName>`* Ce préfixe correspond à l' Région AWS endroit où la fonction a été créée. Ce préfixe fait toujours partie du nom du groupe de journaux, même dans les autres Régions où la fonction est invoquée.
- Si vous spécifiez un nom de groupe de journaux personnalisé, tel que *`/MyLogGroup`*, Lambda@Edge n'ajoutera pas le préfixe de Région. Le nom du groupe de journaux reste le même dans toutes les autres Régions où la fonction est invoquée.

> **Note**
>
> Si vous créez un groupe de journaux personnalisé et spécifiez le même nom que le nom par défaut `/aws/lambda/`*`<FunctionName>`*, Lambda@Edge ajoute le préfixe `us-east-1` au nom de la fonction.

Outre la personnalisation du nom du groupe de journaux, les fonctions Lambda@Edge prennent en charge les formats de journal JSON et en texte brut, ainsi que le filtrage au niveau du journal. Pour plus d'informations, consultez Configuration de commandes de journalisation avancées pour la fonction Lambda dans le Guide du développeur AWS Lambda .

> **Note**
>
> Lambda@Edge limite les journaux en fonction du volume de la demande et de la taille des journaux.

Vous devez consulter les fichiers CloudWatch journaux dans la région appropriée pour voir les fichiers journaux de vos fonctions Lambda @Edge. Pour voir les régions dans lesquelles votre fonction Lambda @Edge est exécutée, consultez les graphiques des métriques de la fonction dans la CloudFront console. Les métriques sont affichées pour chaque région . Sur la même page, vous pouvez choisir une région et afficher les fichiers journaux pour cette région afin de pouvoir rechercher des problèmes.

Pour en savoir plus sur l'utilisation des CloudWatch journaux avec les fonctions Lambda @Edge, consultez les rubriques suivantes :

- Pour plus d'informations sur l'affichage des graphiques dans la section Surveillance de la CloudFront console, consultezthe section called “Surveillez CloudFront les métriques avec Amazon CloudWatch”.
- Pour plus d'informations sur les autorisations requises pour envoyer des données à CloudWatch Logs, consultezthe section called “Définition des rôles et autorisations IAM”.
- Pour plus d'informations sur l'ajout de la journalisation à une fonction Lambda, consultez Journalisation des fonctions AWS Lambda dans Node.js ou Journalisation des fonctions AWS Lambda dans Python dans le Guide du développeur AWS Lambda .
- Pour plus d'informations sur CloudWatch les quotas de journaux (anciennement appelés limites), consultez la section Quotas de CloudWatch journaux dans le guide de l'utilisateur Amazon CloudWatch Logs.

CloudFront Journaux de fonctions

Si le code d'une CloudFront fonction contient des `console.log()` instructions, CloudFront Functions envoie automatiquement ces lignes de journal à CloudWatch Logs. S'il n'y a aucune `console.log()` déclaration, rien n'est envoyé à CloudWatch Logs.

CloudFront Functions crée toujours des flux de journaux dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`), quel que soit l'emplacement périphérique sur lequel la fonction a été exécutée. Le nom du flux de journal est au format `YYYY/M/D/`*`UUID`*.

Le nom du groupe de journaux utilise le format suivant :

- Pour CloudFront les fonctions au niveau du comportement du cache, le format est `/aws/cloudfront/function/`*`<FunctionName>`*
- Pour les CloudFront fonctions au niveau de la distribution (fonctions de connexion), le format est `/aws/cloudfront/connection-function/`*`<FunctionName>`*

*`<FunctionName>`*Il s'agit du nom que vous avez donné à la fonction lorsque vous l'avez créée.

Example Demandes des spectateurs

Voici un exemple de message de journal envoyé à CloudWatch Logs. Chaque ligne commence par un identifiant qui identifie de manière unique une CloudFront demande. Le message commence par

une START ligne qui inclut l'ID CloudFront de distribution et se termine par une END ligne. Entre les lignes START et END se trouvent les lignes de journal générées par les instructions `console.log()` de la fonction.

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== START DistributionID:
 E3E5D42GADAXZZ
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== Example function log output
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== END
```

Example Demandes de connexion

Voici un exemple de message de journal envoyé à CloudWatch Logs. Chaque ligne commence par un identifiant qui identifie de manière unique une CloudFront demande. Le message commence par une START ligne qui inclut l'ID CloudFront de distribution et se termine par une END ligne. Entre les lignes START et END se trouvent les lignes de journal générées par les instructions `console.log()` de la fonction.

```
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== START DistributionID:
 E3E5D42GADA123
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== 1.2.3.4
U7b4hR_RaxMADupvKAvr8_m9gsGXvioUggLV5Oyq-vmAtH8HADpjhw== END
```

> **Note**
>
> CloudFront Functions envoie des journaux CloudWatch uniquement pour les fonctions de la `LIVE` phase qui s'exécutent en réponse aux demandes et réponses de production. Lorsque vous testez une fonction, CloudFront elle n'envoie aucun journal à CloudWatch. Le résultat du test contient des informations sur les erreurs, l'utilisation du calcul et les journaux de fonctionnement (`console.log()`instructions), mais ces informations ne sont pas envoyées à CloudWatch.

CloudFront Functions utilise un rôle lié à un service Gestion des identités et des accès AWS (IAM) pour envoyer les journaux aux CloudWatch journaux de votre compte. Un rôle lié à un service est un rôle IAM directement associé à un Service AWS. Les rôles liés au service sont prédéfinis par le service et incluent toutes les autorisations dont le service a besoin Services AWS pour appeler d'autres personnes à votre place. CloudFront Functions utilise le rôle AWSServiceRoleForCloudFrontLoggerlié au service. Pour plus d'informations sur ce rôle, consultez

the section called “Service-linked rôles pour Lambda @Edge” (Lambda@Edge utilise le même rôle lié au service).

Lorsqu'une fonction échoue en raison d'une erreur de validation ou d'exécution, les informations sont enregistrées dans des journaux standard et des journaux d'accès en temps réel. Pour obtenir des informations précises sur l’erreur, consultez les champs `x-edge-result-type`, `x-edge-response-result-type` et `x-edge-detailed-result-type`.

Journalisation des appels CloudFront d'API Amazon à l'aide AWS CloudTrail

CloudFront est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API CloudFront sous forme d'événements. Les appels capturés incluent des appels provenant de la CloudFront console et des appels de code vers les opérations de l' CloudFront API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite CloudFront, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l’identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d’identification d’utilisateur root ou d’utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d’identification de sécurité temporaires d’un rôle ou d’un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du Console de gestion AWS sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

> **Note**
>
> CloudFront est un service mondial. CloudTrail enregistre des événements CloudFront dans la région de l'est des États-Unis (Virginie du Nord). Pour plus d'informations, consultez Événements de services mondiaux dans le Guide de l'utilisateur AWS CloudTrail .
> Si vous utilisez des informations d'identification de sécurité temporaires en utilisant AWS Security Token Service, les appels vers les points de terminaison régionaux`us-west-2`, tels que, sont connectés CloudTrail à la région appropriée.
> Pour plus d'informations sur les CloudFront points de terminaison, consultez la section CloudFront Points de terminaison et quotas dans le. Références générales AWS

CloudFront événements de données dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource (par exemple, lecture ou écriture dans une CloudFront distribution). Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités à fort volume. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de CloudFront ressources à l'aide de la CloudTrail console ou AWS CLI des opérations de CloudTrail l'API. Pour plus d'informations sur la façon de journaliser les événements de données, consultez Journalisation des événements de données avec la Console de gestion AWS et Journalisation des événements de données avec l' AWS Command Line Interface dans le Guide de l'utilisateur AWS CloudTrail .

Le tableau suivant répertorie les types de CloudFront ressources pour lesquels vous pouvez enregistrer des événements de données. La colonne Type d'événement de données (console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur resources.type indique la **`resources.type`** valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide du ou. AWS CLI CloudTrail APIs La CloudTrail colonne Données APIs enregistrées indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`	• DeleteKeys • DescribeKeyValueStore • GetKey • ListKeys • PutKeys • UpdateKeys

Vous pouvez configurer des sélecteurs d'événements avancés pour filtrer les champs `eventName`, `readOnly` et `resources.ARN` afin de ne journaliser que les événements importants pour vous. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelector dans la Référence des API AWS CloudTrail .

CloudFront événements de gestion dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Amazon CloudFront enregistre toutes les opérations CloudFront du plan de contrôle en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de CloudFront contrôle Amazon auxquelles CloudFront se connecte CloudTrail, consultez le Amazon CloudFront API Reference.

CloudFront exemples d'événements

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

Table des matières

- Exemple : UpdateDistribution
- Exemple : UpdateKeys

Exemple : UpdateDistribution

L'exemple suivant montre un CloudTrail événement illustrant l'UpdateDistributionopération.

Pour les appels à l' CloudFront API, `eventSource` c'est`cloudfront.amazonaws.com`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:role-session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/role-session-name",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-02-02T19:23:50Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-02-02T19:26:01Z",
    "eventSource": "cloudfront.amazonaws.com",
    "eventName": "UpdateDistribution",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "52.94.133.137",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.0.0 Safari/537.36",
    "requestParameters": {
        "distributionConfig": {
            "defaultRootObject": "",
            "aliases": {
                "quantity": 3,
                "items": [
                    "alejandro_rosalez.awsps.myinstance.com",
                    "cross-testing.alejandro_rosalez.awsps.myinstance.com",
```

```
                    "*.alejandro_rosalez.awsps.myinstance.com"
                ]
            },
            "cacheBehaviors": {
                "quantity": 0,
                "items": []
            },
            "httpVersion": "http2and3",
            "originGroups": {
                "quantity": 0,
                "items": []
            },
            "viewerCertificate": {
                "minimumProtocolVersion": "TLSv1.2_2021",
                "cloudFrontDefaultCertificate": false,
                "aCMCertificateArn": "arn:aws:acm:us-east-1:111122223333:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                "sSLSupportMethod": "sni-only"
            },
            "webACLId": "arn:aws:wafv2:us-east-1:111122223333:global/webacl/testing-
acl/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "customErrorResponses": {
                "quantity": 0,
                "items": []
            },
            "logging": {
                "includeCookies": false,
                "prefix": "",
                "enabled": false,
                "bucket": ""
            },
            "priceClass": "PriceClass_All",
            "restrictions": {
                "geoRestriction": {
                    "restrictionType": "none",
                    "quantity": 0,
                    "items": []
                }
            },
            "isIPV6Enabled": true,
            "callerReference": "1578329170895",
            "continuousDeploymentPolicyId": "",
            "enabled": true,
            "defaultCacheBehavior": {
```

```
                "targetOriginId": "d111111abcdef8",
                "minTTL": 0,
                "compress": false,
                "maxTTL": 31536000,
                "functionAssociations": {
                    "quantity": 0,
                    "items": []
                },
                "trustedKeyGroups": {
                    "quantity": 0,
                    "items": [],
                    "enabled": false
                },
                "smoothStreaming": false,
                "fieldLevelEncryptionId": "",
                "defaultTTL": 86400,
                "lambdaFunctionAssociations": {
                    "quantity": 0,
                    "items": []
                },
                "viewerProtocolPolicy": "redirect-to-https",
                "forwardedValues": {
                    "cookies": {"forward": "none"},
                    "queryStringCacheKeys": {
                        "quantity": 0,
                        "items": []
                    },
                    "queryString": false,
                    "headers": {
                        "quantity": 1,
                        "items": ["*"]
                    }
                },
                "trustedSigners": {
                    "items": [],
                    "enabled": false,
                    "quantity": 0
                },
                "allowedMethods": {
                    "quantity": 2,
                    "items": [
                        "HEAD",
                        "GET"
                    ],
```

```
                "cachedMethods": {
                    "quantity": 2,
                    "items": [
                        "HEAD",
                        "GET"
                    ]
                }
            }
        },
        "staging": false,
        "origins": {
            "quantity": 1,
            "items": [
                {
                    "originPath": "",
                    "connectionTimeout": 10,
                    "customOriginConfig": {
                        "originReadTimeout": 30,
                        "hTTPSPort": 443,
                        "originProtocolPolicy": "https-only",
                        "originKeepaliveTimeout": 5,
                        "hTTPPort": 80,
                        "originSslProtocols": {
                            "quantity": 3,
                            "items": [
                                "TLSv1",
                                "TLSv1.1",
                                "TLSv1.2"
                            ]
                        }
                    },
                    "id": "d111111abcdef8",
                    "domainName": "d111111abcdef8.cloudfront.net",
                    "connectionAttempts": 3,
                    "customHeaders": {
                        "quantity": 0,
                        "items": []
                    },
                    "originShield": {"enabled": false},
                    "originAccessControlId": ""
                }
            ]
        },
        "comment": "HIDDEN_DUE_TO_SECURITY_REASONS"
```

```
        },
        "id": "EDFDVBD6EXAMPLE",
        "ifMatch": "E1RTLUR9YES76O"
    },
    "responseElements": {
        "distribution": {
            "activeTrustedSigners": {
                "quantity": 0,
                "enabled": false
            },
            "id": "EDFDVBD6EXAMPLE",
            "domainName": "d111111abcdef8.cloudfront.net",
            "distributionConfig": {
                "defaultRootObject": "",
                "aliases": {
                    "quantity": 3,
                    "items": [
                        "alejandro_rosalez.awsps.myinstance.com",
                        "cross-testing.alejandro_rosalez.awsps.myinstance.com",
                        "*.alejandro_rosalez.awsps.myinstance.com"
                    ]
                },
                "cacheBehaviors": {"quantity": 0},
                "httpVersion": "http2and3",
                "originGroups": {"quantity": 0},
                "viewerCertificate": {
                    "minimumProtocolVersion": "TLSv1.2_2021",
                    "cloudFrontDefaultCertificate": false,
                    "aCMCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                    "sSLSupportMethod": "sni-only",
                    "certificateSource": "acm",
                    "certificate": "arn:aws:acm:us-east-1:111122223333:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "webACLId": "arn:aws:wafv2:us-east-1:111122223333:global/webacl/
testing-acl/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
                "customErrorResponses": {"quantity": 0},
                "logging": {
                    "includeCookies": false,
                    "prefix": "",
                    "enabled": false,
                    "bucket": ""
                },
```

```
                "priceClass": "PriceClass_All",
                "restrictions": {
                    "geoRestriction": {
                        "restrictionType": "none",
                        "quantity": 0
                    }
                },
                "isIPV6Enabled": true,
                "callerReference": "1578329170895",
                "continuousDeploymentPolicyId": "",
                "enabled": true,
                "defaultCacheBehavior": {
                    "targetOriginId": "d111111abcdef8",
                    "minTTL": 0,
                    "compress": false,
                    "maxTTL": 31536000,
                    "functionAssociations": {"quantity": 0},
                    "trustedKeyGroups": {
                        "quantity": 0,
                        "enabled": false
                    },
                    "smoothStreaming": false,
                    "fieldLevelEncryptionId": "",
                    "defaultTTL": 86400,
                    "lambdaFunctionAssociations": {"quantity": 0},
                    "viewerProtocolPolicy": "redirect-to-https",
                    "forwardedValues": {
                        "cookies": {"forward": "none"},
                        "queryStringCacheKeys": {"quantity": 0},
                        "queryString": false,
                        "headers": {
                            "quantity": 1,
                            "items": ["*"]
                        }
                    },
                    "trustedSigners": {
                        "enabled": false,
                        "quantity": 0
                    },
                    "allowedMethods": {
                        "quantity": 2,
                        "items": [
                            "HEAD",
                            "GET"
```

```
                    ],
                    "cachedMethods": {
                        "quantity": 2,
                        "items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                }
            },
            "staging": false,
            "origins": {
                "quantity": 1,
                "items": [
                    {
                        "originPath": "",
                        "connectionTimeout": 10,
                        "customOriginConfig": {
                            "originReadTimeout": 30,
                            "hTTPSPort": 443,
                            "originProtocolPolicy": "https-only",
                            "originKeepaliveTimeout": 5,
                            "hTTPPort": 80,
                            "originSslProtocols": {
                                "quantity": 3,
                                "items": [
                                    "TLSv1",
                                    "TLSv1.1",
                                    "TLSv1.2"
                                ]
                            }
                        },
                        "id": "d111111abcdef8",
                        "domainName": "d111111abcdef8.cloudfront.net",
                        "connectionAttempts": 3,
                        "customHeaders": {"quantity": 0},
                        "originShield": {"enabled": false},
                        "originAccessControlId": ""
                    }
                ]
            },
            "comment": "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "aliasICPRecordals": [
```

```
                {
                    "cNAME": "alejandro_rosalez.awsps.myinstance.com",
                    "iCPRecordalStatus": "APPROVED"
                },
                {
                    "cNAME": "cross-testing.alejandro_rosalez.awsps.myinstance.com",
                    "iCPRecordalStatus": "APPROVED"
                },
                {
                    "cNAME": "*.alejandro_rosalez.awsps.myinstance.com",
                    "iCPRecordalStatus": "APPROVED"
                }
            ],
            "aRN": "arn:aws:cloudfront::111122223333:distribution/EDFDVBD6EXAMPLE",
            "status": "InProgress",
            "lastModifiedTime": "Feb 2, 2024 7:26:01 PM",
            "activeTrustedKeyGroups": {
                "enabled": false,
                "quantity": 0
            },
            "inProgressInvalidationBatches": 0
        },
        "eTag": "E1YHBLAB2BJY1G"
    },
    "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
    "eventID": "5ab02562-0fc5-43d0-b7b6-90293example",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "apiVersion": "2020_05_31",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "cloudfront.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


Exemple : UpdateKeys

L'exemple suivant montre un CloudTrail événement illustrant l'UpdateKeysopération.

Pour les appels à l' CloudFront KeyValueStore API, le `eventSource` est `edgekeyvaluestore.amazonaws.com` au lieu de`cloudfront.amazonaws.com`.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:role-session-name",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/role-session-name",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2023-11-01T23:41:14Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-01T23:41:28Z",
    "eventSource": "edgekeyvaluestore.amazonaws.com",
    "eventName": "UpdateKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.235.183.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/121.0.0.0 Safari/537.36,
    "requestParameters": {
        "kvsARN": "arn:aws:cloudfront::111122223333:key-value-store/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "ifMatch": "KV3O6B1CX531EBP",
        "deletes": [
            {"key": "key1"}
        ]
    },
    "responseElements": {
        "itemCount": 0,
        "totalSizeInBytes": 0,
```

```
        "eTag": "KVDC9VEVZ71ZGO"
    },
    "requestID": "5ccf104c-acce-4ea1-b7fc-73e33example",
    "eventID": "a0b1b5c7-906c-439d-9925-90293example",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::CloudFront::KeyValueStore",
            "ARN": "arn:aws:cloudfront::111122223333:key-value-store/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "111122223333.cloudfront-kvs.global.api.aws"
    }
}
```


Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Suivez les modifications de configuration avec AWS Config

Pour enregistrer et évaluer les configurations de vos AWS ressources, vous pouvez utiliser AWS Config, qui vous fournit une vue détaillée de la configuration de vos distributions. Elle indique comment les ressources sont liées entre elles et comment elles ont été configurées dans le passé, afin que vous puissiez examiner les changements au fil du temps.

Vous pouvez également l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à vos paramètres CloudFront de distribution. Vous pouvez capturer les modifications apportées aux états de distribution, catégories de tarifs, origines, paramètres de restriction géographique et configurations Lambda@Edge.

> **Note**
>
> AWS Config n'enregistre pas de balises clé-valeur pour les distributions CloudFront en streaming.

Table des matières

- Configurez AWS Config avec CloudFront
- Afficher l'historique CloudFront de configuration
- Évaluer les CloudFront configurations à l'aide de AWS Config règles

Configurez AWS Config avec CloudFront

Lors de la configuration AWS Config, vous pouvez choisir d'enregistrer toutes les AWS ressources prises en charge ou de n'enregistrer que certaines ressources spécifiques, par exemple en enregistrant les modifications pour CloudFront uniquement. Pour obtenir la liste des CloudFront ressources prises en charge, consultez la CloudFront section Amazon de la rubrique Types de ressources pris en charge dans le Guide du AWS Config développeur.

> **Remarques**
>
> - Pour suivre les modifications de configuration apportées à votre CloudFront distribution, vous devez vous connecter à la CloudFront console dans l'est des États-Unis (Virginie du Nord) Région AWS.
> - Il se peut qu'il y ait un retard dans l'enregistrement des ressources avec AWS Config. AWS Config enregistre les ressources uniquement après les avoir découvertes.

Console

À configurer AWS Config avec CloudFront

1. Connectez-vous à la AWS Config console Console de gestion AWS et ouvrez-la.
2. Choisir Get Started Now (Démarrer maintenant).
3. Sur la page Paramètres, pour Types de ressources à enregistrer, spécifiez les types de AWS ressources que vous AWS Config souhaitez enregistrer. Si vous souhaitez enregistrer

uniquement les CloudFront modifications, choisissez Types spécifiques, puis, sous CloudFront, choisissez la distribution ou la distribution en streaming dont vous souhaitez suivre les modifications.

Pour ajouter ou modifier les distributions dont vous souhaitez effectuer le suivi, choisissez Settings (Paramètres) sur la gauche, à la fin de votre configuration initiale.

4. Spécifiez les options supplémentaires requises pour AWS Config : configurer une notification, spécifier un emplacement pour les informations de configuration et ajouter des règles pour évaluer les types de ressources.

Pour plus d'informations, consultez la section Configuration à l' AWS Config aide de la console dans le guide du AWS Config développeur.

AWS CLI

Pour configurer à CloudFront l' AWS Config aide du AWS CLI, consultez la section Configuration à l' AWS Config aide de la AWS CLI dans le guide du AWS Config développeur.

AWS Config API

Pour configurer CloudFront l'utilisation AWS Config de l' AWS Config API, consultez le fonctionnement de l' StartConfigurationRecorderAPI dans la référence de l'AWS Config API.

Afficher l'historique CloudFront de configuration

Une fois que l'enregistrement des modifications de configuration de vos distributions a AWS Config commencé, vous pouvez obtenir l'historique de configuration de toutes les distributions pour lesquelles vous avez configuré les distributionsCloudFront.

Vous pouvez consulter les historiques de configuration de la manière suivante.

Console

Pour chaque ressource enregistrée, vous pouvez visualiser une page chronologique fournissant un historique des détails de configuration. Pour visualiser cette page, choisissez l’icône grise dans la colonne Chronologie de configuration de la page Hôtes dédiés.

Pour plus d'informations, consultez la section Affichage des détails de configuration dans la AWS Config console dans le guide du AWS Config développeur.

AWS CLI

Pour obtenir la liste de toutes vos distributions, exécutez la list-discovered-resourcescommande, comme indiqué dans l'exemple suivant.

```
aws configservice list-discovered-resources --resource-type
 AWS::CloudFront::Distribution
```

Pour obtenir les détails de configuration d'une distribution pour un intervalle de temps spécifique, exécutez la get-resource-config-historycommande.

Pour plus d'informations, consultez Afficher les détails de configuration à l'aide de la CLI dans le Guide du développeur AWS Config .

AWS Config API

Pour obtenir la liste de toutes vos distributions, utilisez l'opération ListDiscoveredResourcesAPI.

Pour obtenir les détails de configuration d'une distribution pour un intervalle de temps spécifique, utilisez l'opération GetResourceConfigHistoryAPI. Pour plus d'informations, consultez la Référence des API AWS Config.

Évaluer les CloudFront configurations à l'aide de AWS Config règles

Vous pouvez évaluer les configurations par rapport aux configurations souhaitées à l'aide de AWS Config règles. Par exemple, AWS Config Rules vous aide à évaluer si vos CloudFront ressources sont conformes aux meilleures pratiques de sécurité courantes. Vous pouvez choisir des règles gérées telles que la politique d'affichage HTTPS, l'activation SNI, l'OAC, le basculement d'origine activé, le AWS WAF WebACL ou les politiques de AWS Shield Advanced ressources à déclencher lorsque la configuration change.

Les règles gérées peuvent exécuter des évaluations périodiquement, à la fréquence que vous choisissez. AWS Firewall Manager s'appuie sur AWS Config des alertes et des corrections automatiques. Pour plus d'informations, consultez les sections Évaluation des ressources à l'aide de AWS Config règles et Liste des règles AWS Config gérées dans le Guide du AWS Config développeur.

La sécurité sur Amazon CloudFront

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : elle AWS est responsable de la protection de l'infrastructure qui exécute AWS les services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party les auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon CloudFront, consultez la section AWS Services concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation CloudFront. Les rubriques suivantes vous montrent comment procéder à la configuration CloudFront pour atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos CloudFront ressources.

- Protection des données sur Amazon CloudFront— Protégez vos données en transit et au repos.
- Gestion des identités et des accès pour Amazon CloudFront— Gérez l'accès aux CloudFront ressources et aux autorisations.
- Journalisation et surveillance sur Amazon CloudFront— Suivez les demandes et surveillez l'état de santé de vos distributions.
- Validation de conformité pour Amazon CloudFront— Comprenez comment CloudFront répond aux programmes de conformité.
- Résilience dans Amazon CloudFront— En savoir plus sur la résilience de l' CloudFront infrastructure.

- Sécurité de l'infrastructure sur Amazon CloudFront— En savoir plus sur la sécurité de l'infrastructure pour CloudFront.

Rubriques

- Protection des données sur Amazon CloudFront
- Gestion des identités et des accès pour Amazon CloudFront
- Journalisation et surveillance sur Amazon CloudFront
- Validation de conformité pour Amazon CloudFront
- Résilience dans Amazon CloudFront
- Sécurité de l'infrastructure sur Amazon CloudFront

Protection des données sur Amazon CloudFront

Le modèle de responsabilité AWS https://aws.amazon.com/compliance/shared-responsibility-model/ s'applique à la protection des données sur Amazon CloudFront. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble des AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la FAQ sur la confidentialité des données et les conditions légales de la région . Pour plus d'informations sur la protection des données en Europe, consultez le Centre du règlement général sur la protection des données (RGPD).

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour enregistrer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le Guide de AWS CloudTrail l'utilisateur.

- Utilisez des solutions de AWS cryptage, ainsi que tous les contrôles de sécurité par défaut qui s'y trouvent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec CloudFront ou Services AWS utilisez la console, l'API ou les AWS kits de développement logiciel. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Amazon CloudFront propose plusieurs options que vous pouvez utiliser pour sécuriser le contenu diffusé :

- Configurer les connexions HTTPS.
- Configurez le chiffrement au niveau du champ pour fournir une sécurité supplémentaire pour des données spécifiques pendant le transit.
- Restreindre l'accès au contenu de manière à ce que seules des personnes spécifiques ou des personnes dans une zone spécifique puissent l'afficher.

Les rubriques suivantes expliquent les options plus en détail.

Rubriques

- Chiffrement en transit
- Chiffrement au repos
- Restreindre l'accès au contenu

Chiffrement en transit

Pour crypter vos données pendant le transit, vous configurez Amazon de manière CloudFront à ce que les spectateurs utilisent le protocole HTTPS pour demander vos fichiers, afin que les connexions soient cryptées lors des communications CloudFront avec les spectateurs. Vous pouvez également configurer CloudFront l'utilisation du protocole HTTPS pour récupérer les fichiers depuis votre origine, afin que les connexions soient chiffrées lorsque CloudFront vous communiquez avec votre origine.

Pour plus d'informations, consultez Utilisez le protocole HTTPS avec CloudFront.

Field-level le chiffrement ajoute une couche de sécurité supplémentaire au même titre que le protocole HTTPS qui vous permet de protéger des données spécifiques tout au long du traitement du système afin que seules certaines applications puissent les consulter. En configurant le chiffrement au niveau des champs dans CloudFront, vous pouvez télécharger en toute sécurité les informations sensibles soumises par les utilisateurs sur vos serveurs Web. Les informations sensibles fournies par vos clients sont chiffrées en périphérie plus près de l'utilisateur. Il reste chiffré sur l'ensemble de votre pile d'applications, ce qui garantit que seules les applications qui ont besoin des données et disposent des informations d'identification nécessaires pour les déchiffrer peuvent le faire.

Pour plus d'informations, consultez Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.

Les points de terminaison `cloudfront.amazonaws.com` et les points de terminaison de `cloudfront-fips.amazonaws.com` l' CloudFront API n'acceptent que le trafic HTTPS. Cela signifie que lorsque vous envoyez et recevez des informations à l'aide de l' CloudFront API, vos données sont toujours cryptées en transit. Ces données incluent les configurations de distribution, les politiques de cache et les politiques de demande d'origine, les groupes de clés et les clés publiques, ainsi que le code de fonction dans CloudFront Functions. En outre, toutes les demandes envoyées aux points de terminaison de l' CloudFront API sont signées avec des AWS informations d'identification et connectées. AWS CloudTrail

Le code de fonction et la configuration dans CloudFront Functions sont toujours chiffrés en transit lorsqu'ils sont copiés vers les points de présence périphériques (POP) et entre les autres emplacements de stockage utilisés par CloudFront.

Chiffrement au repos

Le code de fonction et la configuration dans CloudFront Functions sont toujours stockés dans un format crypté sur les POPs de l'emplacement périphérique et dans les autres emplacements de stockage utilisés par CloudFront.

Restreindre l'accès au contenu

De nombreuses entreprises qui distribuent du contenu via Internet veulent limiter l'accès aux documents, données professionnelles, flux multimédias ou contenus destinés à un sous-ensemble d'utilisateurs. Pour diffuser ce contenu en toute sécurité à l'aide d'Amazon CloudFront, vous pouvez effectuer l'une ou plusieurs des opérations suivantes :

Utiliser des cookies ou des URL signés

Vous pouvez restreindre l'accès au contenu destiné à certains utilisateurs, par exemple les utilisateurs qui ont payé des frais, en diffusant ce contenu privé à l' CloudFront aide d'URL signées ou de cookies signés. Pour plus d'informations, consultez Offre de contenu privé avec des URL et des cookies signés.

Restriction de l'accès au contenu dans les compartiments Amazon S3

Si vous limitez l'accès à votre contenu en utilisant, par exemple, des URL CloudFront signées ou des cookies signés, vous ne souhaiterez pas non plus que les internautes consultent les fichiers en utilisant l'URL directe du fichier. Au lieu de cela, vous souhaitez qu'ils accèdent aux fichiers uniquement en utilisant l'URL CloudFront , afin que vos protections fonctionnent.

Si vous utilisez un compartiment Amazon S3 comme origine d'une CloudFront distribution, vous pouvez configurer un contrôle d'accès à l'origine (OAC) qui permet de restreindre l'accès au compartiment S3. Pour plus d'informations, consultez the section called “Restriction de l'accès à une origine Amazon S3”.

Restreindre l'accès au contenu diffusé par un Application Load Balancer

Lorsque vous utilisez CloudFront un équilibreur de charge d'application dans Elastic Load Balancing comme origine, vous pouvez le configurer CloudFront pour empêcher les utilisateurs d'accéder directement à l'équilibreur de charge d'application. Cela permet aux utilisateurs d'accéder à l'équilibreur de charge d'application uniquement via CloudFront, en vous assurant de bénéficier des avantages de son utilisation CloudFront. Pour plus d'informations, consultez Restriction de l'accès aux Application Load Balancers.

Utiliser les AWS WAF ACL Web

Vous pouvez utiliser AWS WAF un service de pare-feu d'application Web pour créer une liste de contrôle d'accès Web (ACL Web) afin de restreindre l'accès à votre contenu. En fonction des conditions que vous spécifiez, telles que les adresses IP d'où proviennent les demandes ou les valeurs des chaînes de requête, CloudFront répond aux demandes soit avec le contenu

demandé, soit avec un code d'état HTTP 403 (Interdit). Pour plus d’informations, consultez Utilisation AWS WAF protections.

Utiliser une restriction géographique

Vous pouvez utiliser une restriction géographique, également appelée blocage géographique, pour empêcher les utilisateurs situés à des emplacements géographiques spécifiques d'accéder au contenu que vous desservez via une distribution CloudFront. Il existe plusieurs options au choix lorsque vous configurez des restrictions géographiques. Pour de plus amples informations, veuillez consulter Restriction de la distribution géographique de votre contenu.

Gestion des identités et des accès pour Amazon CloudFront

Gestion des identités et des accès AWS (IAM) permet à un Service AWS administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (possède des autorisations) à utiliser CloudFront les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l’accès à l’aide de politiques
- Comment Amazon CloudFront travaille avec IAM
- Identity-based exemples de politiques pour Amazon CloudFront
- AWS politiques gérées pour Amazon CloudFront
- Utilisez des rôles liés à un service pour CloudFront
- Résoudre les problèmes d' CloudFront identité et d'accès à Amazon

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résoudre les problèmes d' CloudFront identité et d'accès à Amazon)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment Amazon CloudFront travaille avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Identity-based exemples de politiques pour Amazon CloudFront)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identité. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), de l'authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une interface de ligne de commande pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à l' Services AWS aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de votre annuaire d'entreprise, de votre fournisseur d'identité Web ou Directory Service qui accède à l' Services AWS aide d'informations d'identification provenant

d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le Guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle utilisateur à un rôle IAM (console) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous associez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques en ligne (intégrées directement dans une identité unique) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon CloudFront travaille avec IAM

Avant d'utiliser IAM pour gérer l'accès à CloudFront, découvrez quelles fonctionnalités IAM sont disponibles. CloudFront

Fonctionnalités IAM que vous pouvez utiliser avec Amazon CloudFront

Fonctionnalité IAM	CloudFront soutien
Identity-based politiques	Oui
Resource-based politiques	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non

Fonctionnalité IAM	CloudFront soutien
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Transfert des sessions d'accès (FAS)	Non
Rôles du service	Non
Service-linked rôles	Oui

Pour obtenir une vue d'ensemble de la façon dont CloudFront les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Identity-based politiques pour CloudFront

Prend en charge les politiques basées sur l'identité : oui

Identity-based les politiques sont des documents de politique d'autorisations JSON que vous pouvez joindre à une identité, telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Identity-based exemples de politiques pour CloudFront

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Identity-based exemples de politiques pour Amazon CloudFront

Resource-based politiques au sein de CloudFront

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de stratégie JSON que vous joignez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour CloudFront

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des CloudFront actions, consultez la section Actions définies par Amazon CloudFront dans la référence d'autorisation de service.

Les actions de stratégie en CloudFront cours utilisent le préfixe suivant avant l'action :

```
cloudfront
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "cloudfront:action1",
      "cloudfront:action2"
```

```
        ]
```

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Identity-based exemples de politiques pour Amazon CloudFront

Ressources politiques pour CloudFront

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de CloudFront ressources et de leurs ARN, consultez la section Ressources définies par Amazon CloudFront dans le Service Authorization Reference. Pour savoir quelles actions vous permettent de spécifier l'ARN de chaque ressource, consultez la section Actions définies par Amazon CloudFront.

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Identity-based exemples de politiques pour Amazon CloudFront

Clés de condition de politique pour CloudFront

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser des politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition,

tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, consultez les clés contextuelles de conditions AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de CloudFront condition, consultez la section Clés de condition pour Amazon CloudFront dans la référence d'autorisation de service. Pour savoir avec quelles actions et quelles ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par Amazon CloudFront.

Pour consulter des exemples de politiques CloudFront basées sur l'identité, consultez. Identity-based exemples de politiques pour Amazon CloudFront

ACL dans CloudFront

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec CloudFront

Prend en charge ABAC (identifications dans les politiques) : partiellement

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à celle de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration

de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

CloudFront prend en charge ABAC pour les CloudFront ressources qui prennent en charge les balises, telles que les distributions, les locataires ou les magasins de confiance.

Utilisation d'informations d'identification temporaires avec CloudFront

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès de courte durée aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Sessions d'accès direct pour CloudFront

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour CloudFront

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut entraîner une interruption des CloudFront fonctionnalités. Modifiez les rôles de service CloudFront uniquement lorsque cela vous est indiqué.

Service-linked rôles pour CloudFront

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre compte Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

CloudFront utilise des rôles liés aux services pour effectuer des actions à votre place. Pour plus d'informations sur la création ou la gestion de rôles CloudFront liés à un service, consultez. Utilisez des rôles liés à un service pour CloudFront Pour plus d'informations sur la création ou la gestion des rôles liés à un service Lambda@Edge, consultez Service-linked rôles pour Lambda @Edge.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne des Service-linked rôles. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Identity-based exemples de politiques pour Amazon CloudFront

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources CloudFront. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par CloudFront, notamment le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon CloudFront dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Autorisations d'accès CloudFront par programmation
- Autorisations requises pour utiliser la CloudFront console
- Exemples de politiques gérées par le client

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer des CloudFront ressources sur votre compte, y accéder ou en supprimer. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations avec le moindre privilège — Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par le AWS client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un outil spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger une authentification multifacteur (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root Compte AWS, activez l'authentification multifacteur pour

renforcer la sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations nécessaires pour effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Autorisations d'accès CloudFront par programmation

Voici une politique d'autorisations. Le `Sid`, ou ID de l'instruction, est facultatif.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "AllowAllCloudFrontPermissions",
         "Effect": "Allow",
         "Action": ["cloudfront:*"],
         "Resource": "*"
      }
   ]
}
```

La politique accorde des autorisations pour effectuer toutes les CloudFront opérations, ce qui est suffisant pour accéder CloudFront par programmation. Si vous utilisez la console pour y accéder CloudFront, consultezAutorisations requises pour utiliser la CloudFront console.

Pour obtenir la liste des actions et l'ARN que vous spécifiez pour accorder ou refuser l'autorisation d'utiliser chaque action, consultez la section Actions, ressources et clés de condition pour Amazon CloudFront dans la référence d'autorisation de service.

Autorisations requises pour utiliser la CloudFront console

Pour accorder un accès complet à la CloudFront console, vous devez accorder les autorisations conformément à la politique d'autorisations suivante :

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:*",
            "cloudwatch:DescribeAlarms",
            "cloudwatch:PutMetricAlarm",
            "cloudwatch:GetMetricStatistics",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets",
            "s3:PutBucketPolicy"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Voici pourquoi les autorisations sont obligatoires :

`acm:ListCertificates`

Lorsque vous créez et mettez à jour des distributions à l'aide de la CloudFront console et que vous CloudFront souhaitez configurer pour exiger le protocole HTTPS entre le CloudFront visualiseur CloudFront et l'origine, vous pouvez consulter une liste de certificats ACM.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`cloudfront:*`

Vous pouvez effectuer toutes les CloudFront actions.

`cloudwatch:DescribeAlarms` et **`cloudwatch:PutMetricAlarm`**

Vous permet de créer et de visualiser CloudWatch des alarmes dans la CloudFront console. Voir aussi `sns:ListSubscriptionsByTopic` et `sns:ListTopics`.

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console CloudFront.

`cloudwatch:GetMetricStatistics`

Faisons CloudFront le rendu CloudWatch des métriques dans la CloudFront console.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`elasticloadbalancing:DescribeLoadBalancers`

Lorsque vous créez et mettez à jour des distributions, vous pouvez consulter la liste des équilibreurs de charge Elastic Load Balancing dans la liste des origines disponibles.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`iam:ListServerCertificates`

Lorsque vous créez et mettez à jour des distributions à l'aide de la CloudFront console et que vous souhaitez configurer CloudFront pour exiger le protocole HTTPS entre le CloudFront visualiseur CloudFront et l'origine, vous pouvez consulter une liste de certificats dans le magasin de certificats IAM.

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`s3:ListAllMyBuckets`

Lorsque vous créez et mettez à jour des distributions, vous pouvez effectuer les opérations suivantes :

- Afficher une liste des compartiments S3 dans la liste des origines disponibles
- Afficher une liste de compartiments S3 dans lesquels vous pouvez enregistrer les journaux d'accès

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`S3:PutBucketPolicy`

Lorsque vous créez ou mettez à jour les distributions qui limitent l'accès aux compartiments S3, permet à un utilisateur de mettre à jour la stratégie de compartiment pour accorder l'accès à

l'identité d'accès à l'origine CloudFront. Pour plus d'informations, consultez the section called "Utilisation d'une identité d'accès d'origine (héritée, non recommandée)".

Cette autorisation n'est pas requise si vous n'utilisez pas la CloudFront console.

`sns:ListSubscriptionsByTopic` et **`sns:ListTopics`**

Lorsque vous créez des CloudWatch alarmes dans la CloudFront console, vous pouvez choisir un sujet SNS pour les notifications.

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console CloudFront.

`waf:GetWebACL` et **`waf:ListWebACLs`**

Vous pouvez consulter la liste des ACL AWS WAF Web dans la CloudFront console.

Ces autorisations ne sont pas nécessaires si vous n'utilisez pas la console CloudFront.

Permission-only actions pour la CloudFront console

Vous pouvez effectuer les CloudFront actions suivantes sur la page CloudFront Security Savings Bundle. Les actions d'API suivantes ne sont pas destinées à être appelées par votre code et ne sont pas incluses dans les AWS SDK AWS CLI et.

Action	Description
`CreateSavingsPlan`	Accorde l'autorisation de créer un nouveau Savings Plan (plan d'épargne).
`GetSavingsPlan`	Accorde l'autorisation d'obtenir un Savings Plan (plan d'épargne).
`ListRateCards`	Autorise la mise en CloudFront vente des cartes tarifaires pour le compte.
`ListSavingsPlans`	Accorde l'autorisation de répertorier les Savings Plans dans le compte.
`ListUsages`	Autorise l' CloudFront utilisation de la liste.
`UpdateSavingsPlan`	Accorde l'autorisation de mettre à jour un Savings plan.

Remarques

- Pour plus d'informations sur les plans CloudFront d'épargne, consultez la section CloudFront Security Savings Bundle des CloudFront FAQ Amazon.
- Si vous créez un plan d'épargne pour CloudFront et que vous souhaitez le supprimer ultérieurement, contactez AWS Support.

Exemples de politiques gérées par le client

Vous pouvez créer vos propres politiques IAM personnalisées pour autoriser les actions d' CloudFront API. Vous pouvez attacher ces politiques personnalisées aux utilisateurs ou groupes IAM qui nécessitent les autorisations spécifiées. Ces politiques fonctionnent lorsque vous utilisez l' CloudFront API, les AWS SDK ou le AWS CLI. Les exemples suivants présentent des autorisations pour quelques cas d'utilisation courants. Pour la politique qui accorde à un utilisateur un accès complet à CloudFront, consultezAutorisations requises pour utiliser la CloudFront console.

Exemples

- Exemple 1 : Autoriser l'accès en lecture à toutes les distributions
- Exemple 2 : Créer, mettre à jour et supprimer des distributions
- Exemple 3 : Autoriser la création et l'inventaire des invalidations
- Exemple 4 : autoriser la création d’une distribution

Exemple 1 : Autoriser l'accès en lecture à toutes les distributions

La politique d'autorisations suivante accorde à l'utilisateur les autorisations nécessaires pour afficher toutes les distributions dans la CloudFront console :

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
```

```
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Exemple 2 : Créer, mettre à jour et supprimer des distributions

Avec la politique d'autorisations suivante, vous pouvez créer, mettre à jour et supprimer des distributions à l'aide de la CloudFront console :

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "acm:ListCertificates",
            "cloudfront:CreateDistribution",
            "cloudfront:DeleteDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
```

```
            "cloudfront:UpdateDistribution",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets",
            "s3:PutBucketPolicy"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

L'autorisation `cloudfront:ListCloudFrontOriginAccessIdentities` permet aux utilisateurs d'accorder automatiquement à une identité d'accès à l'origine existante l'autorisation d'accès aux objets dans un compartiment Amazon S3. Si vous souhaitez également que les utilisateurs puissent créer des identités d'accès à l'origine, vous devez également accorder l'autorisation `cloudfront:CreateCloudFrontOriginAccessIdentity`.

Exemple 3 : Autoriser la création et l'inventaire des invalidations

Avec la politique d'autorisations suivante, vous pouvez créer et répertorier des invalidations. Il inclut l'accès en lecture aux CloudFront distributions, car vous créez et visualisez des invalidations en affichant d'abord les paramètres d'une distribution :

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
```

```
         "Action":[
            "acm:ListCertificates",
            "cloudfront:GetDistribution",
            "cloudfront:GetStreamingDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListCloudFrontOriginAccessIdentities",
            "cloudfront:CreateInvalidation",
            "cloudfront:GetInvalidation",
            "cloudfront:ListInvalidations",
            "elasticloadbalancing:DescribeLoadBalancers",
            "iam:ListServerCertificates",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
            "waf:GetWebACL",
            "waf:ListWebACLs"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Exemple 4 : autoriser la création d'une distribution

La politique d'autorisation suivante accorde à l'utilisateur l'autorisation de créer et de répertorier des distributions dans la CloudFront console. Pour l'action `CreateDistribution`, spécifiez le caractère générique (*) pour la `Resource` lieu d'un caractère générique pour l'ARN de distribution (`arn:aws:cloudfront::123456789012:distribution/*`). Pour en savoir plus sur l'élément `Resource`, consultez Éléments de politique JSON IAM : Resource dans le Guide de l'utilisateur IAM.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "cloudfront:CreateDistribution",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "cloudfront:ListDistributions",
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour Amazon CloudFront

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour Créer des politiques IAM gérées par le client qui fournissent aux utilisateurs uniquement les autorisations dont ils ont besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont les plus susceptibles de mettre à jour une politique gérée par AWS lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles autorisations deviennent disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité,

il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

Rubriques

- AWS politique gérée : CloudFrontReadOnlyAccess
- AWS politique gérée : CloudFrontFullAccess
- AWS politique gérée : AWSCloudFrontLogger
- AWS politique gérée : AWSLambdaReplicator
- AWS politique gérée : AWSCloudFrontVPCOriginServiceRolePolicy
- CloudFront mises à jour de AWS stratégies gérées

AWS politique gérée : CloudFrontReadOnlyAccess

Vous pouvez associer la politique CloudFrontReadOnlyAccess à vos identités IAM. Cette politique autorise les autorisations en lecture seule pour les ressources. CloudFront Il autorise également des autorisations en lecture seule pour d'autres ressources de AWS service associées à la CloudFront console et visibles dans celle-ci. CloudFront

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `cloudfront:Describe*`— Permet aux directeurs d'obtenir des informations sur les métadonnées relatives aux CloudFront ressources.
- `cloudfront:Get*`— Permet aux responsables d'obtenir des informations détaillées et des configurations pour les CloudFront ressources.
- `cloudfront:List*`— Permet aux directeurs d'obtenir des listes de CloudFront ressources.
- `cloudfront-keyvaluestore:Describe*` - permet aux principaux d'obtenir des informations sur le magasin de clés-valeurs.
- `cloudfront-keyvaluestore:Get*` - permet aux principaux d'obtenir des informations détaillées et des configurations pour le magasin de clés-valeurs.
- `cloudfront-keyvaluestore:List*` - permet aux principaux d'obtenir des listes des magasins de clés-valeurs.

- `acm:DescribeCertificate` : permet aux principaux d'obtenir des informations sur un certificat ACM.
- `acm:ListCertificates` – Permet aux entités principales d'obtenir une liste de certificats ACM.
- `iam:ListServerCertificates` – Permet aux entités principales d'obtenir une liste des certificats de serveur stockés dans IAM.
- `route53:List*` – Permet aux entités principales d'obtenir des listes de ressources Route 53.
- `waf:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `waf:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.
- `wafv2:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `wafv2:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.
- `pricingplanmanager:GetSubscription`— Permet aux principaux d'accéder en lecture seule aux informations relatives aux abonnements aux plans tarifaires.
- `pricingplanmanager:ListSubscriptions`— Permet aux principaux d'accéder en lecture seule à la liste des abonnements aux plans tarifaires.
- `ec2:DescribeIpamPools`— Permet aux principaux d'obtenir des informations détaillées sur vos pools IPAM.
- `ec2:GetIpamPoolCidrs`— Permet aux principaux d'approvisionner les CIDR dans un pool IPAM.

Pour voir les autorisations de cette stratégie, consultez CloudFrontReadOnlyAccess dans le AWS Guide de référence des stratégies gérées par.

AWS politique gérée : CloudFrontFullAccess

Vous pouvez associer la politique CloudFrontFullAccess à vos identités IAM. Cette politique autorise les autorisations administratives sur les CloudFront ressources. Il autorise également des autorisations en lecture seule pour d'autres ressources de AWS service associées à la CloudFront console et visibles dans celle-ci. CloudFront

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `s3:ListAllMyBuckets` – Permet aux entités principales d'obtenir une liste de tous les compartiments Amazon S3.
- `acm:DescribeCertificate` : permet aux principaux d'obtenir des informations sur un certificat ACM.
- `acm:ListCertificates` – Permet aux entités principales d'obtenir une liste de certificats ACM.
- `acm:RequestCertificate` : permet aux principaux de demander des certificats gérés à ACM.
- `cloudfront:*`— Permet aux principaux d'effectuer toutes les actions sur toutes les CloudFront ressources.
- `cloudfront-keyvaluestore:*` - permet aux principaux d'effectuer toutes les actions sur le magasin de clés-valeurs.
- `iam:ListServerCertificates` – Permet aux entités principales d'obtenir une liste des certificats de serveur stockés dans IAM.
- `waf:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `waf:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.
- `waf:CreateWebACLs`— Permet aux principaux de créer une ACL Web dans AWS WAF.
- `wafv2:ListWebACLs` – Permet aux entités principales d'obtenir une liste des ACL Web dans AWS WAF.
- `wafv2:GetWebACL` – Permet aux entités principales d'obtenir des informations détaillées sur les ACL Web dans AWS WAF.
- `kinesis:ListStreams` – Permet aux entités principales d'obtenir une liste des Amazon Kinesis streams.
- `elasticloadbalancing:DescribeLoadBalancers` - permet aux principaux d'obtenir des informations détaillées sur les équilibreurs de charge dans Elastic Load Balancing.
- `kinesis:DescribeStream` – Permet aux entités principales d'obtenir des informations détaillées sur un flux Kinesis.
- `iam:ListRoles` – Permet aux entités principales d'obtenir une liste des rôles dans IAM.
- `pricingplanmanager:AssociateResourcesToSubscription`- Permet aux principaux d'associer des ressources à un abonnement. Cela permet aux ressources d'être couvertes par le plan tarifaire de l'abonnement.
- `pricingplanmanager:CancelSubscription`- Permet aux principaux d'annuler un abonnement existant.

- `pricingplanmanager:CancelSubscriptionChange`- Permet aux principaux d'annuler une modification en attente d'un abonnement existant, telle qu'une mise à niveau du plan, avant que la modification ne soit appliquée.
- `pricingplanmanager:CreateSubscription`- Permet aux donneurs d'ordre de créer un abonnement à un plan tarifaire.
- `pricingplanmanager:DisassociateResourcesFromSubscription`- Permet aux principaux de supprimer l'association entre les ressources et un abonnement existant.
- `pricingplanmanager:UpdateSubscription`- Permet aux clients principaux de modifier un abonnement existant, par exemple en modifiant le plan tarifaire.
- `pricingplanmanager:GetSubscription`— Permet aux principaux d'accéder en lecture seule aux informations relatives aux abonnements aux plans tarifaires.
- `pricingplanmanager:ListSubscriptions`— Permet aux principaux d'accéder en lecture seule à la liste des abonnements aux plans tarifaires.
- `pricingplanmanager:ApprovePaidSubscription`— Permet aux mandants d'approuver un abonnement payant et de commencer à facturer.
- `freetier:GetAccountPlanState`— Permet aux principaux d'obtenir l'état du plan AWS Free Tier pour le compte, utilisé pour déterminer l'éligibilité aux plans tarifaires forfaitaires.
- `cloudwatch:GetMetricData`— Permet aux donneurs d'ordre de récupérer les données CloudWatch métriques, utilisées pour déterminer l'éligibilité aux plans tarifaires forfaitaires.
- `shield:ListProtections`— Permet aux donneurs d'ordre de répertorier les protections du AWS Shield, utilisées pour déterminer l'éligibilité aux plans tarifaires forfaitaires.
- `ec2:DescribeInstances` - permet aux principaux d’obtenir des informations détaillées sur les instances dans Amazon EC2.
- `ec2:DescribeInternetGateways` - permet aux principaux d’obtenir des informations détaillées sur les passerelles Internet dans Amazon EC2.
- `ec2:DescribeIpamPools`— Permet aux principaux d'obtenir des informations détaillées sur vos pools IPAM.
- `ec2:GetIpamPoolCidrs`— Permet aux principaux d'approvisionner les CIDR dans un pool IPAM.

Pour voir les autorisations de cette stratégie, consultez CloudFrontFullAccess dans le AWS Guide de référence des stratégies gérées par.

> **Note**
>
> La CloudFrontFullAccesspolitique inclut l'`pricingplanmanager:ApprovePaidSubscription`autorisation, qui engage votre compte à débiter des frais pour les forfaits payants qui ne peuvent pas être annulés avant la fin de la période de facturation en cours. Pour les flux de travail automatisés, tels que les pipelines de déploiement, les agents ou les rôles de service, nous recommandons une politique délimitée qui accorde des autorisations `pricingplanmanager:CreateSubscription` sans`pricingplanmanager:ApprovePaidSubscription`, afin qu'un humain autorise la facturation. Pour plus d'informations, consultez Commencer à utiliser l' PricingPlanManager API.

> **Important**
>
> Si vous souhaitez CloudFront créer et enregistrer des journaux d'accès, vous devez accorder des autorisations supplémentaires. Pour de plus amples informations, veuillez consulter Permissions.

AWS politique gérée : AWSCloudFrontLogger

Vous ne pouvez pas associer la AWSCloudFrontLoggerpolitique à vos identités IAM. Cette politique est associée à un rôle lié à un service qui permet d' CloudFront effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter the section called “Service-linked rôles pour Lambda @Edge”.

Cette politique permet CloudFront d'envoyer des fichiers journaux à Amazon CloudWatch. Pour obtenir des détails sur les autorisations incluses dans cette politique, consultez the section called “Service-linked autorisations de rôle pour l' CloudFront enregistreur”.

Pour voir les autorisations de cette stratégie, consultez AWSCloudFrontLogger dans le AWS Guide de référence des stratégies gérées par.

AWS politique gérée : AWSLambdaReplicator

Vous ne pouvez pas associer la AWSLambdaReplicatorpolitique à vos identités IAM. Cette politique est associée à un rôle lié à un service qui permet d' CloudFront effectuer des actions en votre nom.

Pour de plus amples informations, veuillez consulter the section called “Service-linked rôles pour Lambda @Edge”.

Cette politique permet CloudFront de créer, de supprimer et de désactiver des fonctions AWS Lambda pour répliquer des fonctions Lambda @Edge dans. Régions AWS Pour obtenir des détails sur les autorisations incluses dans cette politique, consultez the section called “Service-linked autorisations de rôle pour le réplicateur Lambda”.

Pour voir les autorisations de cette stratégie, consultez AWSLambdaReplicator dans le AWS Guide de référence des stratégies gérées par.

AWS politique gérée : AWSCloudFrontVPCOriginServiceRolePolicy

Vous ne pouvez pas associer AWSCloudFrontVPCOriginServiceRolePolicy à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet d' CloudFront effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisez des rôles liés à un service pour CloudFront.

Cette politique permet CloudFront de gérer les interfaces réseau élastiques et les groupes de sécurité EC2 en votre nom. Pour obtenir des détails sur les autorisations incluses dans cette politique, consultez the section called “Autorisations de rôle liées à un service pour VPC Origins CloudFront”.

Pour voir les autorisations de cette stratégie, consultez AWSCloudFrontVPCOriginServiceRolePolicy dans le AWS Guide de référence des stratégies gérées par.

CloudFront mises à jour de AWS stratégies gérées

Consultez les détails des mises à jour des politiques AWS gérées CloudFront depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du CloudFront document.

Modifier	Description	Date
CloudFrontFullAccess : mise à jour de la politique existante	CloudFront a ajouté de nouvelles autorisations pour l'éligibilité au plan tarifaire forfaitaire et l'approbation des abonnements.	29 juillet 2026

Modifier	Description	Date
	Les nouvelles autorisations permettent aux principaux d'utiliser les `shield:ListProtections` actions `pricingplanmanager:ApprovePaidSubscription` `freetier:GetAccountPlanState` ,`cloudwatch:GetMetricData` , et.	
CloudFrontReadOnlyAccess : mise à jour de la politique existante	CloudFront a ajouté de nouvelles autorisations pour Amazon EC2. Les nouvelles autorisations permettent aux directeurs d'utiliser les `ec2:GetIpamPoolCidrs` actions `ec2:DescribeIpamPools` et.	24 novembre 2025
CloudFrontFullAccess : mise à jour de la politique existante	CloudFront a ajouté de nouvelles autorisations pour Amazon EC2. Les nouvelles autorisations permettent aux directeurs d'utiliser les `ec2:GetIpamPoolCidrs` actions `ec2:DescribeIpamPools` et.	24 novembre 2025

Modifier	Description	Date
CloudFrontFullAccess : mise à jour de la politique existante	CloudFront a ajouté une nouvelle autorisation pour créer une ressource AWS WAF ACL et a ajouté des autorisations de création, de mise à jour, de suppression et de lecture à AWS Pricing Plan Manager.	18 novembre 2025
CloudFrontFullAccess : mise à jour de la politique existante	CloudFront a ajouté une nouvelle autorisation pour créer une ressource AWS WAF ACL et a ajouté des autorisations de création, de mise à jour, de suppression et de lecture à AWS Pricing Plan Manager.	18 novembre 2025
CloudFrontReadOnlyAccess : mise à jour de la politique existante	CloudFront a ajouté de nouvelles autorisations pour un accès en lecture seule au AWS Pricing Plan Manager.	18 novembre 2025
CloudFrontReadOnlyAccess : mise à jour de la politique existante	CloudFront a ajouté de nouvelles autorisations pour un accès en lecture seule au AWS Pricing Plan Manager.	18 novembre 2025
CloudFrontReadOnlyAccess : mise à jour de la politique existante	CloudFront ajout d'une nouvelle autorisation pour ACM. La nouvelle autorisation permet aux principaux d’obtenir des informations sur un certificat ACM.	28 avril 2025

Modifier	Description	Date
CloudFrontFullAccess : mise à jour de la politique existante	CloudFront a ajouté de nouvelles autorisations pour ACM. Les nouvelles autorisations permettent aux principaux d'obtenir des informations sur un certificat ACM et de demander un certificat géré à ACM.	28 avril 2025
CloudFrontFullAccess : mise à jour de la politique existante	CloudFront a ajouté de nouvelles autorisations pour Amazon EC2 et Elastic Load Balancing. Les nouvelles autorisations permettent d' CloudFron t obtenir des informations détaillées sur les équilibreurs de charge dans Elastic Load Balancing et sur les instances et les passerelles Internet dans Amazon EC2.	20 novembre 2024
AWSCloudFrontVPCOr iginServiceRolePolicy : nouvelle politique	CloudFront a ajouté une nouvelle politique. Cette politique permet CloudFront de gérer les interfaces réseau élastiques et les groupes de sécurité EC2 en votre nom.	20 novembre 2024

Modifier	Description	Date
CloudFrontReadOnlyAccess et CloudFrontFullAccess : mise à jour de deux politiques existantes.	CloudFront a ajouté de nouvelles autorisations pour les magasins à valeur clé. Les nouvelles autorisations permettent aux utilisateurs d'obtenir des informations sur les magasins de clés-valeurs et d'agir sur ceux-ci.	19 décembre 2023
CloudFrontReadOnlyAccess : mise à jour d'une politique existante	CloudFront a ajouté une nouvelle autorisation pour décrire CloudFront les fonctions. Cette autorisation permet à l'utilisateur, au groupe ou au rôle de lire des informations et des métadonnées sur une fonction, mais pas sur le code de la fonction.	8 septembre 2021
CloudFront a commencé à suivre les modifications	CloudFront a commencé à suivre les modifications apportées AWS à ses politique s gérées.	8 septembre 2021

Utilisez des rôles liés à un service pour CloudFront

Amazon CloudFront utilise des rôles Gestion des identités et des accès AWS liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. CloudFront Les rôles liés au service sont prédéfinis par CloudFront et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration CloudFront car vous n'avez pas à ajouter manuellement les autorisations nécessaires. CloudFront définit les autorisations associées à ses

rôles liés aux services et, sauf indication contraire, seul CloudFront peut assumer ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos CloudFront ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour VPC Origins CloudFront

CloudFront VPC Origins utilise le rôle lié au service nommé AWSServiceRoleForCloudFrontVPCOrigin— Permet CloudFront de gérer les interfaces réseau élastiques et les groupes de sécurité EC2 en votre nom.

Le rôle lié à un service AWSServiceRoleForCloudFrontVPCOrigin approuve les services suivants pour endosser le rôle :

- `vpcorigin.cloudfront.amazonaws.com`

La politique d'autorisation de rôle nommée AWSCloud Front VPCOrigin ServiceRolePolicy permet à CloudFront VPC Origins d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `ec2:CreateNetworkInterface` sur `arn:aws:ec2:*:*:network-interface/*`
- Action : `ec2:CreateNetworkInterface` sur `arn:aws:ec2:*:*:subnet/*` et `arn:aws:ec2:*:*:security-group/*`
- Action : `ec2:CreateSecurityGroup` sur `arn:aws:ec2:*:*:security-group/*`
- Action : `ec2:CreateSecurityGroup` sur `arn:aws:ec2:*:*:vpc/*`
- Action : `ec2:ModifyNetworkInterfaceAttribute`, `ec2:DeleteNetworkInterface`, `ec2:DeleteSecurityGroup`, `ec2:AssignIpv6Addresses` et `ec2:UnassignIpv6Addresses` sur `supported AWS resources that have the aws:ResourceTag/aws.cloudfront.vpcorigin tag enabled`
- Action : `ec2:DescribeNetworkInterfaces`, `ec2:DescribeSecurityGroups`, `ec2:DescribeInstances`, `ec2:DescribeInternetGateways`, `ec2:DescribeSubnets`,

`ec2:DescribeRegions` et `ec2:DescribeAddresses` sur `all AWS resources that the actions support`

- Action : `ec2:CreateTags` sur `arn:aws:ec2:*:*:security-group/*` et `arn:aws:ec2:*:*:network-interface/*`
- Action : `elasticloadbalancing:DescribeLoadBalancers`, `elasticloadbalancing:DescribeListeners` et `elasticloadbalancing:DescribeTargetGroups` sur `all AWS resources that the actions support`

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour VPC Origins CloudFront

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une origine VPC dans le Console de gestion AWS, le ou l' AWS API AWS CLI, CloudFront VPC Origins crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une origine VPC, VPC Origins crée à CloudFront nouveau le rôle lié au service pour vous.

Modifier un rôle lié à un service pour VPC Origins CloudFront

CloudFront VPC Origins ne vous permet pas de modifier le rôle lié au AWSServiceRoleForCloudFrontVPCOrigin service. Après avoir créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour VPC Origins CloudFront

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le CloudFront service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources CloudFront VPC Origins utilisées par AWSServiceRoleForCloudFrontVPCOrigin

- Supprimez les ressources de l'origine VPC de votre compte.
  - La suppression des ressources CloudFront de votre compte peut prendre un certain temps. Si vous ne pouvez pas supprimer immédiatement le rôle lié au service, attendez et réessayez.

Pour supprimer manuellement le rôle lié au service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForCloudFrontVPCOrigin service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les CloudFront rôles liés au service VPC Origins

CloudFront VPC Origins ne prend pas en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Vous pouvez utiliser le rôle AWSServiceRoleForCloudFrontVPCOrigin dans les régions suivantes :

Nom de la région	Identité de la région	Support dans CloudFront
USA Est (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1 (sauf l'AZ usw1-az2)	Oui
USA Ouest (Oregon)	us-west-2	Oui
Afrique (Le Cap)	af-south-1	Oui
Asie-Pacifique (Hong Kong)	ap-east-1	Oui

Nom de la région	Identité de la région	Support dans CloudFront
Asie-Pacifique (Jakarta)	ap-southeast-3	Oui
Asie-Pacifique (Melbourne)	ap-southeast-4	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Hyderabad)	ap-south-2	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Oui
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1 (sauf l'AZ apne1-az3)	Oui
Canada (Centre)	ca-central-1 (sauf l'AZ cac1-az3)	Oui
Canada-Ouest (Calgary)	ca-west-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Milan)	eu-south-1	Oui
Europe (Paris)	eu-west-3	Oui
Europe (Espagne)	eu-south-2	Oui
Europe (Stockholm)	eu-north-1	Oui
Europe (Zurich)	eu-central-2	Oui

Nom de la région	Identité de la région	Support dans CloudFront
Israël (Tel Aviv)	il-central-1	Oui
Moyen-Orient (Bahreïn)	me-south-1	Oui
Moyen-Orient (EAU)	me-central-1	Oui
Amérique du Sud (São Paulo)	sa-east-1	Oui

Résoudre les problèmes d' CloudFront identité et d'accès à Amazon

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec un CloudFront IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans CloudFront
- Je ne suis pas autorisé à exécuter iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes CloudFront ressources

Je ne suis pas autorisé à effectuer une action dans CloudFront

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `cloudfront:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudfront:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `cloudfront:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à exécuter iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à CloudFront.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans CloudFront. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes CloudFront ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises CloudFront en charge, consultezComment Amazon CloudFront travaille avec IAM.

- Pour savoir comment donner accès à vos ressources par l'intermédiaire de celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS qui vous appartient dans le Guide de l'utilisateur IAM.
- Pour savoir comment donner accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Journalisation et surveillance sur Amazon CloudFront

La surveillance joue un rôle important dans le maintien de la disponibilité CloudFront et des performances de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller vos CloudFront ressources et votre activité, et répondre aux incidents potentiels :

CloudWatch Alarmes Amazon

À l'aide d' CloudWatch alarmes, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, une notification est envoyée à une rubrique ou AWS Auto Scaling à une politique Amazon SNS. CloudWatch les alarmes n'appellent aucune action lorsqu'une métrique est dans un état particulier. L'état doit avoir changé et avoir été conservé pendant un nombre de périodes spécifié.

Pour de plus amples informations, veuillez consulter Surveillez CloudFront les métriques avec Amazon CloudWatch.

AWS CloudTrail journaux

CloudTrail fournit un enregistrement des actions d'API effectuées par un utilisateur, un rôle ou un AWS service dans CloudFront. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande d'API qui a été faite CloudFront, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour de plus amples informations, veuillez consulter Journalisation des appels CloudFront d'API Amazon à l'aide AWS CloudTrail.

CloudFront journaux standard et journaux d'accès en temps réel

CloudFront les journaux fournissent des informations détaillées sur les demandes adressées à une distribution. Ces journaux sont utiles pour de nombreuses applications. Par exemple, les informations des journaux peuvent être importantes en cas d'audit de sécurité ou des accès.

Pour plus d'informations, consultez Journaux d'accès (journaux standard) et Création et utilisation de configurations de journaux d'accès en temps réel.

Journaux des fonctions de périphérie

Les journaux générés par les fonctions périphériques, CloudFront Functions et Lambda @Edge, sont envoyés directement à Amazon CloudWatch Logs et ne sont stockés nulle part par. CloudFront CloudFront Functions utilise un rôle lié à un service Gestion des identités et des accès AWS (IAM) pour envoyer les journaux générés par les clients directement aux CloudWatch journaux de votre compte.

Pour de plus amples informations, veuillez consulter Journaux des fonctions de périphérie.

CloudFront rapports de console

La CloudFront console inclut divers rapports, notamment le rapport sur les statistiques du cache, le rapport sur les objets populaires et le rapport sur les principaux référents. La plupart des rapports de CloudFront console sont basés sur les données des journaux CloudFront d'accès, qui contiennent des informations détaillées sur chaque demande d'utilisateur CloudFront reçue. Toutefois, vous n'avez pas besoin d'activer les journaux d'accès pour consulter ces rapports.

Pour plus d'informations, consultez Afficher CloudFront les rapports dans la console.

Validation de conformité pour Amazon CloudFront

Third-party les auditeurs évaluent la sécurité et la conformité d'Amazon dans CloudFront le cadre de multiples programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, HIPAA.

Pour obtenir la liste des AWS services concernés par des programmes de conformité spécifiques, consultez la section AWS Services concernés par programme de conformité. Pour obtenir des informations générales, consultez Programmes de conformitéAWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans AWS Artifact.

Votre responsabilité en matière de conformité lors de l'utilisation CloudFront dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide en matière de sécurité et de conformité : ces guides de déploiement abordent les considérations architecturales et fournissent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Architecting for HIPAA Security and Compliance on AWS — Ce livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications. HIPAA-compliant

  Le programme de conformité AWS HIPAA inclut CloudFront (à l'exception de la diffusion de contenu via des POPs CloudFront intégrés) un service éligible à la HIPAA. Si vous avez signé un Business Associate Addendum (BAA) avec AWS, vous pouvez l'utiliser CloudFront (à l'exception de la diffusion de contenu via des POPs CloudFront intégrés) pour diffuser du contenu contenant des informations de santé protégées (PHI). Pour de plus amples informations, consultez Conformité à la loi HIPAA.
- AWS Ressources relatives à la conformité : cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue la conformité de vos configurations de ressources aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub CSPM— Ce AWS service utilise des contrôles de sécurité pour évaluer les configurations des ressources et les normes de sécurité afin de vous aider à vous conformer aux différents cadres de conformité. Pour plus d'informations sur l'utilisation de Security Hub CSPM pour évaluer les CloudFront ressources, consultez les CloudFront contrôles Amazon dans le Guide de l'AWS Security Hub CSPM utilisateur.

CloudFront meilleures pratiques en matière de conformité

Cette section fournit les meilleures pratiques et des recommandations en matière de conformité lorsque vous utilisez Amazon CloudFront pour diffuser votre contenu.

Vous pouvez exécuter PCI-compliant des HIPAA-compliant charges de travail basées sur le modèle de responsabilité AWS partagée. Dans ce cas, nous vous recommandons d'enregistrer vos données

CloudFront d'utilisation des 365 derniers jours à des fins d'audit futurs. Pour journaliser les données d'utilisation, vous pouvez procéder comme suit :

- Activez les journaux d' CloudFront accès. Pour plus d’informations, consultez Journaux d'accès (journaux standard).
- Demandes de capture envoyées à l' CloudFront API. Pour plus d’informations, consultez Journalisation des appels CloudFront d'API Amazon à l'aide AWS CloudTrail.

En outre, consultez ce qui suit pour plus de détails CloudFront sur la conformité aux normes PCI DSS et SOC.

Norme de sécurité des données de l’industrie des cartes de paiement (PCI DSS)

CloudFront (à l'exception de la diffusion de contenu via des PoPs CloudFront intégrés) prend en charge le traitement, le stockage et la transmission des données de carte de crédit par un commerçant ou un fournisseur de services, et a été validé comme étant conforme à la norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI). Pour plus d'informations sur la norme PCI DSS, notamment sur la procédure à suivre pour demander une copie du package de conformité AWS PCI, consultez la section PCI DSS niveau 1.

Pour des raisons de sécurité, nous vous recommandons de ne pas mettre en cache les informations relatives aux cartes de crédit dans les caches CloudFront périphériques. Par exemple, vous pouvez configurer votre origine pour inclure un `Cache-Control:no-cache="` *`field-name`* `"` en-tête dans les réponses contenant des informations de carte de crédit, telles que les quatre derniers chiffres d'un numéro de carte de crédit et les coordonnées du titulaire de la carte.

System and Organization Controls (SOC)

CloudFront (à l'exception de la diffusion de contenu via des POP CloudFront intégrés) est conforme aux mesures de contrôle du système et de l'organisation (SOC), notamment SOC 1, SOC 2 et SOC 3. Les rapports SOC sont des rapports d'examen indépendants réalisés par des tiers qui montrent AWS comment atteindre les principaux contrôles et objectifs de conformité. Ces audits garantissent que les garanties et les procédures appropriées sont en place pour se protéger contre les risques susceptibles d'affecter la sécurité, la confidentialité et la disponibilité des données des clients et des entreprises. Les résultats de ces audits tiers sont disponibles sur le site Web de conformité du AWS SOC, où vous pouvez consulter les rapports publiés pour obtenir plus d'informations sur les contrôles qui soutiennent les AWS opérations et la conformité.

Résilience dans Amazon CloudFront

L'infrastructure mondiale AWS s'articule autour de régions et de zones de disponibilité AWS. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les régions et les zones de disponibilité AWS, consultez AWS Infrastructure mondiale.

Basculement d'origine CloudFront

Outre la prise en charge de l'infrastructure globale AWS, Amazon CloudFront propose une fonctionnalité de basculement d'origine pour vous permettre de répondre à vos besoins en matière de résilience des données. CloudFront est un service mondial qui fournit votre contenu via un réseau mondial de centres de données appelé emplacements périphériques ou points de présence (POP). Si votre contenu n'est pas déjà mis en cache dans un emplacement périphérique, CloudFront l'extrait d'une origine que vous avez identifiée comme étant la source de la version définitive du contenu.

Vous pouvez améliorer la résilience et augmenter la disponibilité pour des scénarios spécifiques en configurant CloudFront avec le basculement d'origine. Pour commencer, vous créez un groupe d'origine dans lequel vous indiquez une origine principale pour CloudFront plus une seconde origine. CloudFront bascule automatiquement vers la deuxième origine lorsque l'origine principale renvoie des réponses d'échec de code d'état HTTP spécifiques. Pour plus d'informations, consultez Optimisez la haute disponibilité grâce au basculement CloudFront d'origine.

Sécurité de l'infrastructure sur Amazon CloudFront

En tant que service géré, Amazon CloudFront est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et la manière de AWS protéger l'infrastructure, consultez AWS Cloud Security. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans Security Pillar AWS Well-Architected Framework.

Vous utilisez des appels d'API AWS publiés pour accéder CloudFront via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Suites de chiffrement avec une confidentialité directe parfaite (PFS) telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

CloudFront Functions utilise une barrière d'isolation hautement sécurisée entre les AWS comptes, garantissant ainsi la protection des environnements clients contre les attaques par canaux secondaires telles que Spectre et Meltdown. Functions ne peut pas accéder aux données appartenant à d'autres clients ni les modifier. Functions s'exécute dans un processus monothread sur un processeur dédié sans hyper-threading. Quel que soit le point de présence CloudFront périphérique (POP), CloudFront Functions ne dessert qu'un seul client à la fois, et toutes les données spécifiques au client sont effacées entre les exécutions de fonctions.

Résolution des problèmes

Utilisez cette section pour résoudre les problèmes courants que vous pouvez rencontrer lorsque vous configurez Amazon CloudFront pour distribuer votre contenu.

Chaque rubrique fournit des conseils détaillés pour identifier la cause première des problèmes courants ainsi que des instructions détaillées pour les résoudre.

Rubriques

- Résolution des problèmes de distribution
- Résolution des problèmes liés aux codes d'état de réponse aux erreurs dans CloudFront
- Test de charge CloudFront

Résolution des problèmes de distribution

Utilisez les informations ici pour vous aider à diagnostiquer et à corriger les erreurs de certificat, les problèmes d'accès refusé ou d'autres problèmes courants que vous pourriez rencontrer lors de la configuration de votre site Web ou de votre application avec les distributions Amazon CloudFront .

Rubriques

- CloudFront renvoie un Accès refusé error
- CloudFront renvoie un InvalidViewerCertificate erreur lorsque j'essaie d'ajouter un autre nom de domaine
- CloudFront renvoie une erreur d'enregistrement DNS mal configurée lorsque j'essaie d'ajouter un nouveau CNAME
- Je ne peux pas afficher les fichiers de ma distribution
- Message d'erreur : < Certificat : l'identifiant du certificat > est utilisé par CloudFront

CloudFront renvoie un Accès refusé error

Si vous utilisez un compartiment Amazon S3 comme origine de votre CloudFront distribution, un message d'erreur Access Denied (403) peut s'afficher dans les exemples suivants.

Table des matières

- Vous avez indiqué un objet manquant dans l’origine d’Amazon S3

- Votre origine Amazon S3 ne dispose pas des autorisations IAM nécessaires
- Vous utilisez des informations d'identification non valides ou vous ne disposez pas des autorisations nécessaires

Vous avez indiqué un objet manquant dans l'origine d'Amazon S3

Vérifiez que l'objet demandé existe dans votre compartiment. Les noms des objets sont sensibles à la casse. La saisie d'un nom d'objet non valide peut renvoyer un code d'erreur Accès refusé.

Par exemple, si vous suivez le CloudFront didacticiel pour créer une distribution de base, vous créez un compartiment Amazon S3 en tant qu'origine et vous chargez un exemple de `index.html` fichier.

Dans votre navigateur web, si vous entrez `https://d111111abcdef8.cloudfront.net/INDEX.HTML` au lieu de `https://d111111abcdef8.cloudfront.net/index.html`, un message similaire est susceptible de s'afficher, car le fichier `index.html` dans le chemin de l'URL est sensible à la casse.

```
<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>22Q367AHT7Y1ABCD</RequestId>
<HostId>
ABCDE/Vg+7PSNa/d/IfFQ8Fb92TGQ0KH0ZwG5iEKbc6+e06DdMS1ZW+ryB9GFRIVtS66rSSy6So=
</HostId>
</Error>
```

Votre origine Amazon S3 ne dispose pas des autorisations IAM nécessaires

Vérifiez que vous avez sélectionné le bon compartiment Amazon S3 comme domaine et nom d'origine. L'origine (Amazon S3) doit disposer des autorisations appropriées.

Si vous ne spécifiez pas les autorisations appropriées, un message `AccessDenied` peut s'afficher à l'intention de vos utilisateurs.

Lorsque vous distribuez du contenu depuis Amazon S3 et que vous utilisez également AWS Key Management Service (AWS KMS) le chiffrement côté service (SSE-KMS), vous devez spécifier des autorisations IAM supplémentaires pour la clé KMS et le compartiment Amazon S3. Votre CloudFront distribution a besoin de ces autorisations pour utiliser la clé KMS, qui est utilisée pour le chiffrement du compartiment Amazon S3 d'origine.

Les configurations de la politique de compartiment Amazon S3 permettent à la CloudFront distribution de récupérer les objets chiffrés pour la diffusion de contenu.

Pour vérifier les autorisations de votre compartiment Amazon S3 et de votre clé KMS

1. Vérifiez que la clé KMS que vous utilisez est la même que celle utilisée par votre compartiment Amazon S3 pour le chiffrement par défaut. Pour plus d'informations, consultez la section Spécifier le chiffrement côté serveur avec AWS KMS (SSE-KMS) dans le Guide de l'utilisateur d'Amazon Simple Storage Service.
2. Vérifiez que les objets du compartiment sont chiffrés avec la même clé KMS. Vous pouvez sélectionner n'importe quel objet dans le compartiment Amazon S3 et vérifier les paramètres de chiffrement côté serveur pour vérifier l'ARN de la clé KMS.
3. Modifiez la politique du compartiment Amazon S3 pour CloudFront autoriser l'appel de l'opération d'`GetObject`API depuis le compartiment Amazon S3. Pour un exemple de stratégie de compartiment Amazon S3 utilisant un contrôle d'accès d'origine, consultez Accorder l'CloudFront autorisation d'accéder au compartiment S3.
4. Modifiez la politique de clé KMS pour CloudFront autoriser l'exécution des actions vers `Encrypt`Decrypt, et`GenerateDataKey*`. Pour vous aligner sur l'autorisation du moindre privilège, spécifiez un `Condition` élément de sorte que seule la CloudFront distribution spécifiée puisse effectuer les actions répertoriées. Vous pouvez personnaliser la politique en fonction de votre AWS KMS politique existante. Pour obtenir un exemple de stratégie de clé KMS, consultez SSE-KMS.

Si vous utilisez l'identité d'accès d'origine (OAI) au lieu de l'OAC, les autorisations accordées au compartiment Amazon S3 diffèrent légèrement, car vous accordez les autorisations à une identité plutôt qu'au Service AWS. Pour plus d'informations, consultez Attribution à l'identité d'accès d'origine de l'autorisation de lire les fichiers du compartiment Amazon S3.

Si vous ne parvenez toujours pas à afficher vos fichiers dans votre distribution, consultez Je ne peux pas afficher les fichiers de ma distribution.

Vous utilisez des informations d'identification non valides ou vous ne disposez pas des autorisations nécessaires

Un message d'erreur Accès refusé peut apparaître si vous utilisez des AWS SCT informations d'identification incorrectes ou expirées (clé d'accès et clé secrète) ou si votre rôle ou utilisateur IAM n'a pas l'autorisation requise pour effectuer une action sur une CloudFront ressource. Pour plus

d'informations sur les messages d'erreur d'accès refusé, consultez Résolution des problèmes liés aux messages d'erreur d'accès rejeté dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur la façon dont IAM fonctionne avec CloudFront, consultezGestion des identités et des accès pour Amazon CloudFront.

CloudFront renvoie un InvalidViewerCertificate erreur lorsque j'essaie d'ajouter un autre nom de domaine

Si CloudFront un `InvalidViewerCertificate` message d'erreur s'affiche lorsque vous essayez d'ajouter un autre nom de domaine (CNAME) à votre distribution, consultez les informations suivantes pour vous aider à résoudre le problème. Cette erreur peut indiquer que l'un des problèmes suivants doit être résolu avant que vous puissiez correctement ajouter le nom de domaine alternatif.

Les erreurs suivantes sont répertoriées dans l'ordre dans lequel l' CloudFront autorisation d'ajouter un autre nom de domaine est vérifiée. Cela peut vous aider à résoudre les problèmes, car en fonction de l'erreur CloudFront renvoyée, vous pouvez déterminer quelles vérifications ont été effectuées avec succès.

Il n'y a aucun certificat associé à votre distribution.

> Pour ajouter un nom de domaine alternatif (CNAME), vous devez attacher un certificat valide et approuvé à votre distribution. Consultez les exigences, obtenez un certificat valide qui répond à ces exigences, attachez celui-ci à votre distribution, puis réessayez. Pour plus d'informations, consultez Exigences relatives à l'utilisation de noms de domaines alternatifs.

Il y a un trop grand nombre de certificats dans la chaîne de certificats pour le certificat que vous avez attaché.

> Vous pouvez uniquement posséder jusqu'à cinq certificats dans une chaîne de certificats. Réduisez le nombre de certificats dans la chaîne, puis réessayez.

La chaîne de certificats inclut un ou plusieurs certificats qui ne sont pas valides pour la date du jour.

> La chaîne de certificats pour un certificat que vous avez ajouté a un ou plusieurs certificats qui ne sont pas valides, soit parce que le certificat n'est pas encore valide ou parce qu'il a expiré. Vérifiez les champs Not Valid Before (Non valide avant) et Not Valid After (Non valide après) dans les certificats de votre chaîne de certificats pour vous assurer que tous les certificats sont valides en fonction des dates que vous avez répertoriées.

Le certificat que vous avez attaché n’est pas signé par une autorité de certification (CA) approuvée.

Le certificat auquel vous attachez CloudFront pour vérifier un autre nom de domaine ne peut pas être un certificat auto-signé. Il doit être signé par une autorité de certification approuvée. Pour plus d’informations, consultez Exigences relatives à l’utilisation de noms de domaines alternatifs.

Le certificat que vous avez attaché n’est pas formaté correctement

Le nom de domaine et le format d’adresse IP qui sont inclus dans le certificat et le format du certificat lui-même, doivent respecter la norme pour les certificats.

Une erreur CloudFront interne s'est produite.

CloudFront a été bloqué par un problème interne et n'a pas pu effectuer de contrôles de validation pour les certificats. Dans ce scénario, CloudFront renvoie un code d'état HTTP 500 et indique qu'il existe un CloudFront problème interne lié à l'attachement du certificat. Attendez quelques minutes, puis réessayez pour ajouter le nom de domaine alternatif avec le certificat.

Le certificat que vous avez attaché ne couvre pas le nom de domaine alternatif que vous tentez d'ajouter.

Pour chaque nom de domaine alternatif que vous ajoutez, CloudFront vous devez joindre un SSL/TLS certificat valide provenant d'une autorité de certification (CA) fiable qui couvre le nom de domaine, afin de valider votre autorisation d'utilisation. Mettez à jour votre certificat pour inclure un nom de domaine qui couvre le CNAME que vous tentez d'ajouter. Pour plus d’informations et pour obtenir des exemples d’utilisation de noms de domaines avec caractères génériques, consultez Exigences relatives à l’utilisation de noms de domaines alternatifs.

CloudFront renvoie une erreur d'enregistrement DNS mal configurée lorsque j'essaie d'ajouter un nouveau CNAME

Lorsqu'une entrée DNS générique pointe vers une CloudFront distribution, si vous essayez d'ajouter un nouveau CNAME avec un nom plus spécifique, vous risquez de rencontrer l'erreur suivante :

```
One or more aliases specified for the distribution includes an incorrectly configured
 DNS record that points to another CloudFront distribution. You must update the DNS
 record to correct the problem.
```

Cette erreur se produit car l' CloudFront entrée DNS est renvoyée au CNAME et l'entrée DNS générique est renvoyée à une autre distribution.

Pour résoudre ce problème, créez d'abord une autre distribution, puis créez une entrée DNS pointant vers la nouvelle distribution. Enfin, ajoutez le CNAME plus spécifique. Pour plus d'informations sur l'ajout de CNAME, consultez Ajout d'un nom de domaine alternatif.

Je ne peux pas afficher les fichiers de ma distribution

Si vous ne parvenez pas à afficher les fichiers de votre CloudFront distribution, consultez les rubriques suivantes pour découvrir certaines solutions courantes.

Êtes-vous inscrit à la fois à Amazon S3 CloudFront et à Amazon ?

Pour utiliser Amazon CloudFront avec une origine Amazon S3, vous devez vous inscrire à la fois à Amazon S3 CloudFront et à Amazon S3. Pour plus d'informations sur l'inscription à Amazon S3 CloudFront et à Amazon S3, consultezConfigurez votre Compte AWS.

Votre compartiment Amazon S3 et vos autorisations d'objet sont-elles définis correctement ?

Si vous utilisez CloudFront une source Amazon S3, les versions originales de votre contenu sont stockées dans un compartiment S3. Pour diffuser le contenu à vos spectateurs, nous vous recommandons CloudFront d'utiliser Origin Access Control (OAC) pour sécuriser l'accès au compartiment Amazon S3. Cela signifie que votre compartiment S3 n'est accessible que via CloudFront. L'OAC contrôle l'accès des spectateurs et la diffusion sécurisée en utilisant CloudFront. Pour plus d'informations sur l'OAC, consultez the section called "Restriction de l'accès à une origine Amazon S3".

Pour plus d'informations sur la gestion de l'accès à votre compartiment, consultez Blocage de l'accès public à votre stockage Amazon S3 dans le Guide de l'utilisateur Amazon S3.

Les propriétés d'objet et les propriétés de compartiment sont indépendantes. Vous devez accorder, de manière explicite, des privilèges à chaque objet dans Amazon S3. Les objets n'héritent pas des propriétés des compartiments et les propriétés d'objet doivent être définies indépendamment du compartiment.

Votre nom de domaine alternatif (CNAME) est-il configuré correctement ?

Si vous avez déjà un enregistrement CNAME pour votre nom de domaine, mettez-le à jour ou remplacez-le par un nouvel enregistrement qui pointe vers votre nom de domaine de distribution.

Veillez également à ce que votre archive CNAME dirige vers votre nom de domaine de distribution et non pas votre compartiment Amazon S3. Vous pouvez confirmer que l'archive CNAME dans votre système DNS dirige vers votre nom de domaine de distribution. À cette fin, utilisez un outil DNS tel que dig.

L'exemple suivant illustre une demande dig sur un nom de domaine appelé `images.example.com` et la partie appropriée de la réponse. Sous `ANSWER SECTION`, regardez la ligne qui contient `CNAME`. L'enregistrement CNAME de votre nom de domaine est configuré correctement si la valeur sur le côté droit de CNAME est le nom de domaine de votre CloudFront distribution. S'il s'agit de votre case de serveur d'origine Amazon S3 ou d'autre nom de domaine, alors l'archive CNAME est mal définie.

```
[prompt]> dig images.example.com

; <<> DiG 9.3.3rc2 <<> images.example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15917
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 2, ADDITIONAL: 0
;; QUESTION SECTION:
;images.example.com.   IN  A
;; ANSWER SECTION:
images.example.com. 10800 IN CNAME d111111abcdef8.cloudfront.net.
...
...
```

Pour plus d'informations sur les CNAME, consultez Utilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME).

Faites-vous référence à la bonne URL pour votre CloudFront distribution ?

Assurez-vous que l'URL à laquelle vous faites référence utilise le nom de domaine (ou CNAME) de votre CloudFront distribution, et non votre compartiment Amazon S3 ou votre origine personnalisée.

Avez-vous besoin d'aide pour résoudre un problème lié à une origine personnalisée ?

Si vous avez besoin d'aide AWS pour résoudre les problèmes liés à une origine personnalisée, vous AWS devrez probablement inspecter les entrées `X-Amz-Cf-Id` d'en-tête de vos demandes. Si vous n'enregistrez pas déjà ces entrées, il se peut que vous pensiez à le faire à l'avenir. Pour plus d'informations, consultez the section called "Utilisation d'Amazon EC2 (ou autre origine personnalisée)". Pour obtenir plus d'aide, consultez le Centre de support AWS.

Message d'erreur : < Certificat : l'identifiant du certificat > est utilisé par CloudFront

Problème : vous essayez de supprimer un SSL/TLS certificat du magasin de certificats IAM et le message « Certificat : <certificate-id>is being used by » s'affiche CloudFront.

Solution : chaque CloudFront distribution doit être associée soit au CloudFront certificat par défaut, soit à un SSL/TLS certificat personnalisé. Avant de supprimer un SSL/TLS certificat, vous devez soit effectuer une rotation du certificat (remplacer le SSL/TLS certificat personnalisé actuel par un autre SSL/TLS certificat personnalisé), soit revenir à l'utilisation du SSL/TLS CloudFront certificat par défaut. Pour régler ce problème, effectuez les étapes de l'une des procédures suivantes :

- Rotation SSL/TLS des certificats
- Revenir d'un SSL/TLS certificat personnalisé au certificat par défaut CloudFront

Résolution des problèmes liés aux codes d'état de réponse aux erreurs dans CloudFront

Si CloudFront vous demandez un objet à votre origine et que celle-ci renvoie un code d'état HTTP 4xx ou 5xx, il y a un problème de communication entre CloudFront et votre origine.

Cette rubrique inclut également des étapes de dépannage pour ces codes d'état lors de l'utilisation de Lambda @Edge ou de CloudFront Functions.

Les rubriques suivantes fournissent des explications détaillées sur les causes potentielles de ces réponses aux·erreurs et proposent des conseils étape par étape sur la manière de diagnostiquer et de résoudre les problèmes sous-jacents.

Rubriques

- Code d'état HTTP 400 (Requête incorrecte)
- Code d'état HTTP 401 (Accès non autorisé)
- Code d'état HTTP 403 (méthode non valide)
- Code d'état HTTP 403 (Autorisation refusée)
- Code d'état HTTP 404 (Introuvable)
- Code d'état HTTP 412 (échec de condition préalable)
- Code d'état HTTP 500 (Erreur de serveur interne)

- Code d'état HTTP 502 (Passerelle incorrecte)
- Code d'état HTTP 503 (Service non disponible)
- Code d'état HTTP 504 (Délai d'attente de passerelle expiré)

Code d'état HTTP 400 (Requête incorrecte)

CloudFront renvoie 400 requêtes erronées lorsque le client envoie des données non valides dans la demande, telles que du contenu manquant ou incorrect dans la charge utile ou les paramètres. Il peut également s'agir d'une erreur client générique.

L'origine Amazon S3 renvoie une erreur 400

Si vous utilisez une origine Amazon S3 avec votre CloudFront distribution, celle-ci peut envoyer des réponses d'erreur avec le code d'état HTTP 400 Bad Request et un message similaire au suivant :

L'en-tête d'autorisation est mal formé ; la région « *<AWS Region>* » est incorrecte ; elle attend « » *<AWS Region>*

Par exemple :

The authorization header is malformed; the region 'us-east-1' is wrong; expecting 'us-west-2'

Ce problème peut se produire dans le scénario suivant :

1. L'origine de votre CloudFront distribution est un compartiment Amazon S3.
2. Vous avez déplacé le compartiment S3 d'une AWS région à une autre. En d'autres termes, vous avez supprimé le compartiment S3, puis vous en avez créé un nouveau avec le même nom de compartiment, mais dans une AWS région différente de celle dans laquelle se trouvait le compartiment S3 d'origine.

Pour corriger cette erreur, mettez à jour votre CloudFront distribution afin qu'elle trouve le compartiment S3 dans la AWS région actuelle du compartiment.

Pour mettre à jour votre CloudFront distribution

1. Connectez-vous à Console de gestion AWS et ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez la distribution qui génère cette erreur.

3. Choisissez Origins and Origin Groups (Origines et groupes d'origine).
4. Recherchez l'origine du compartiment S3 que vous avez déplacé. Activez la case à cocher en regard de cette origine, puis choisissez Modifier.
5. Choisissez Oui, Modifier. Vous n'avez pas besoin de modifier les paramètres avant de choisir Oui, Modifier.

Une fois ces étapes terminées, CloudFront redéploie votre distribution. Lorsque la distribution est déployée, l'état du Déploiement s'affiche dans la colonne Dernière modification. Quelque temps après la fin du déploiement, vous devriez cesser de recevoir les réponses aux·erreurs `AuthorizationHeaderMalformed`.

L'origine Application Load Balancer renvoie une erreur 400

Si vous utilisez une origine d'application Load Balancer avec votre CloudFront distribution, les causes possibles d'une erreur 400 sont les suivantes :

- Le client a envoyé une demande incorrecte qui ne respecte pas la spécification HTTP.
- L'en-tête de la demande a dépassé 16 Ko par ligne de demande, 16 Ko par en-tête unique ou 64 Ko pour l'ensemble de l'en-tête de la demande.
- Le client a fermé la connexion avant d'envoyer le corps complet de la demande.

Code d'état HTTP 401 (Accès non autorisé)

Un code d'état de réponse 401 Accès non autorisé indique que la demande du client n'a pas été traitée, car elle ne contient pas d'informations d'identification d'authentification valides pour la ressource demandée. Ce code d'état est envoyé avec un en-tête de réponse HTTP `WWW-Authenticate` qui indique comment le client peut redemander la ressource après avoir sollicité des informations d'identification d'authentification auprès de l'utilisateur. Pour plus d'informations, consultez 401 Accès non autorisé.

Dans CloudFront, si votre origine attend un `Authorization` en-tête pour authentifier les demandes, CloudFront doit transmettre l'`Authorization`en-tête à l'origine pour éviter une erreur 401 Unauthorized. Lorsque CloudFront vous transférez une demande d'utilisateur à votre origine, CloudFront supprime certains en-têtes de visionnage par défaut, y compris l'`Authorization`en-tête. Pour vous assurer que votre origine reçoit toujours l'en-tête `Authorization` dans les demandes d'origine, vous disposez des options suivantes :

- Ajoutez l'en-tête `Authorization` à la clé de cache à l'aide d'une stratégie de cache. Tous les en-têtes de la clé de cache sont automatiquement inclus dans les demandes d'origine. Pour plus d'informations, consultez Contrôle de la clé de cache à l'aide d'une politique.
- Ajoutez l'`Authorization`en-tête individuellement dans une politique de demande d'origine. Pour plus d'informations, consultez Contrôle des demandes d'origine à l'aide d'une stratégie.
- Utilisez une politique de demande d'origine qui transmet tous les en-têtes de l'utilisateur à l'origine. CloudFront fournit une politique de demande d'origine gérée pour ce cas d'utilisation, appelée Managed-AllViewer. Pour plus d'informations, consultez Utilisation des stratégies de demande d'origine gérées.

> **Important**
>
> Si vous transférez l'`Authorization`en-tête vers votre origine sans l'inclure dans la clé de cache, assurez-vous que votre origine ne dépend pas de l'`Authorization`en-tête pour contrôler l'accès au contenu mis en cache. Lorsque l'`Authorization`en-tête ne fait pas partie de la clé de cache, CloudFront peut fournir la même réponse en cache aux spectateurs autorisés et non autorisés. Incluez l'`Authorization`en-tête dans la clé de cache à l'aide d'une politique de cache ou désactivez complètement la mise en cache pour les origines qui nécessitent un traitement d'autorisation côté origine.

Pour plus d'informations, voir Comment puis-je configurer CloudFront pour transférer l'en-tête Authorization vers l'origine ?

Code d'état HTTP 403 (méthode non valide)

CloudFront renvoie une erreur 403 (méthode non valide) si vous essayez d'utiliser une méthode HTTP que vous n'avez pas spécifiée dans la CloudFront distribution. Vous pouvez spécifier l'une des options suivantes pour votre distribution :

- CloudFront uniquement les transferts `GET` et les `HEAD` demandes.
- CloudFront transmet uniquement `GETHEAD`, et `OPTIONS` demandes.
- CloudFront transmet `GETHEAD`,`OPTIONS`,`PUT`, `PATCHPOST`, et `DELETE` demande. (Si vous choisissez cette option, vous devrez peut-être restreindre l'accès à votre compartiment Amazon S3 ou à votre origine personnalisée pour éviter que les utilisateurs réalisent des opérations non

autorisées.) Par exemple, vous ne souhaiterez pas toujours que les utilisateurs disposent des autorisations nécessaires pour supprimer des objets de votre origine.

Code d'état HTTP 403 (Autorisation refusée)

Une erreur HTTP 403 signifie que le client n'est pas autorisé à accéder à la ressource demandée. Le client comprend la demande, mais ne peut pas autoriser l'accès de l'utilisateur. Les causes courantes de CloudFront renvoi de ce code d'état sont les suivantes :

Rubriques

- Le CNAME alternatif est mal configuré
- AWS WAF est configuré lors CloudFront de la distribution ou à l'origine
- L'origine personnalisée renvoie une erreur 403
- L'origine Amazon S3 renvoie une erreur 403
- Les restrictions géographiques renvoient une erreur 403
- La configuration d'une URL signée ou d'un cookie signé renvoie une erreur 403
- Les distributions empilées provoquent une erreur 403

Le CNAME alternatif est mal configuré

Vérifiez que vous avez spécifié le bon CNAME pour votre distribution. Pour utiliser un CNAME alternatif au lieu de l' CloudFront URL par défaut :

1. Créez un enregistrement CNAME dans votre DNS pour pointer le CNAME vers l'URL de CloudFront distribution.
2. Ajoutez le CNAME dans votre configuration CloudFront de distribution.

Si vous créez l'enregistrement DNS mais que vous n'ajoutez pas le CNAME dans votre configuration de CloudFront distribution, la requête renvoie une erreur 403. Pour plus d'informations sur la configuration d'un CNAME personnalisé, consultez Utilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME).

AWS WAF est configuré lors CloudFront de la distribution ou à l'origine

Lorsque AWS WAF se trouve entre le client et CloudFront, CloudFront impossible de faire la distinction entre un code d'erreur 403 renvoyé par votre origine et un code d'erreur 403 renvoyé AWS WAF lorsqu'une demande est bloquée.

Pour trouver la source du code d'état 403, vérifiez la règle de votre liste de contrôle d'accès AWS WAF Web (ACL) pour détecter toute demande bloquée. Pour plus d'informations, consultez les rubriques suivantes :

- AWS WAF listes de contrôle d'accès Web (ACL Web)
- Tester et ajuster vos protections AWS WAF

L'origine personnalisée renvoie une erreur 403

Si vous utilisez une origine personnalisée, une erreur 403 peut s'afficher si vous avez une configuration de pare-feu personnalisée à l'origine. Pour résoudre le problème, envoyez la demande directement à l'origine. Si vous pouvez répliquer l'erreur sans cela CloudFront, cela signifie que l'origine est à l'origine de l'erreur 403.

Si l'origine personnalisée provoque l'erreur, consultez les journaux d'origine pour identifier la cause potentielle de l'erreur. Pour plus d'informations, consultez les rubriques de dépannage suivantes :

- Comment résoudre les erreurs HTTP 403 depuis API Gateway ?
- Comment résoudre les erreurs HTTP 403 Interdit d'un Application Load Balancer ?

L'origine Amazon S3 renvoie une erreur 403

Vous pouvez recevoir une erreur 403 pour les raisons suivantes :

- CloudFront n'a pas accès au compartiment Amazon S3. Cette situation peut se produire si l'identité d'accès d'origine (OAI) ou le contrôle d'accès d'origine (OAC) ne sont pas activés pour votre distribution et que le compartiment est privé.
- Le chemin spécifié dans l'URL demandée n'est pas correct.
- L'objet demandé n'existe pas.
- L'en-tête de l'hôte a été transféré avec le point de terminaison de l'API REST. Pour plus d'informations, consultez Spécification d'un compartiment d'en-tête hôte HTTP dans le Guide de l'utilisateur Amazon Simple Storage Service.

- Vous avez configuré des pages d'erreur personnalisées. Pour plus d'informations, consultez Comment CloudFront traiter les erreurs lorsque vous avez configuré des pages d'erreur personnalisées.

Les restrictions géographiques renvoient une erreur 403

Si vous avez activé les restrictions géographiques (également appelées géoblocage) pour empêcher les utilisateurs situés dans des zones géographiques spécifiques d'accéder au contenu que vous distribuez via une CloudFront distribution, les utilisateurs bloqués reçoivent une erreur 403.

Pour plus d'informations, consultez Restriction de la distribution géographique de votre contenu.

La configuration d'une URL signée ou d'un cookie signé renvoie une erreur 403

Si vous avez activé Limiter l'accès aux utilisateurs dans la configuration du comportement de votre distribution, alors les demandes qui n'utilisent pas de cookies signés ou d'URL signées entraînent une erreur 403. Pour plus d'informations, consultez les rubriques suivantes :

- Offre de contenu privé avec des URL et des cookies signés
- Comment résoudre les problèmes liés à une URL signée ou à des cookies signés ? CloudFront

Les distributions empilées provoquent une erreur 403

Si vous avez deux distributions ou plus dans une chaîne de requêtes adressées au point de terminaison d'origine, CloudFront renvoie une erreur 403. Il n'est pas recommandé de mettre une distribution devant une autre distribution.

Code d'état HTTP 404 (Introuvable)

CloudFront renvoie une erreur 404 (introuvable) lorsque le client tente d'accéder à une ressource qui n'existe pas. Si vous recevez cette erreur avec votre CloudFront distribution, les causes les plus courantes sont les suivantes :

- La ressource n'existe pas.
- L'URL est incorrecte.
- L'origine personnalisée renvoie une erreur 404.

- Les pages d'erreur personnalisées renvoient une erreur 404. (N'importe quel code d'erreur peut être traduit en 404.) Pour plus d'informations, consultez Comment CloudFront traiter les erreurs lorsque vous avez configuré des pages d'erreur personnalisées.
- La page d'erreur personnalisée a été supprimée par erreur, ce qui entraîne un code 404, car la demande recherche cette page d'erreur personnalisée supprimée. Pour plus d'informations, consultez Comment traiter CloudFront les erreurs si vous n'avez pas configuré de pages d'erreur personnalisées.
- Chemin d'origine incorrect. Si le chemin d'origine est renseigné, sa valeur est ajoutée au chemin de chaque demande depuis le navigateur avant que la demande ne soit transmise à l'origine. Pour plus d'informations, consultez Chemin d'origine.

Code d'état HTTP 412 (échec de condition préalable)

CloudFront renvoie un code d'erreur 412 (échec de la précondition) lorsque l'accès à la ressource cible a été refusé. Dans certains cas, un serveur est configuré pour accepter les demandes uniquement lorsque certaines conditions sont remplies. Si l'une des conditions spécifiées n'est pas remplie, le serveur n'autorise pas le client à accéder à la ressource donnée. À la place, le serveur renvoie un code d'erreur 412.

Les causes courantes d'une erreur 412 CloudFront sont les suivantes :

- Demandes conditionnelles sur des méthodes autres que `GET` ou `HEAD` lorsque la condition définie par les en-têtes `If-Unmodified-Since` ou `If-None-Match` n'est pas remplie. Dans ce cas, la demande, généralement un téléchargement ou une modification d'une ressource, ne peut pas être effectuée.
- Une condition dans un ou plusieurs champs de demande de l'opération d' CloudFront UpdateDistributionAPI est évaluée comme fausse.

Code d'état HTTP 500 (Erreur de serveur interne)

Un code d'état HTTP 500 (Erreur de serveur interne) indique que le serveur a rencontré une situation inattendue qui l'a empêché de traiter la demande. Les causes courantes de 500 erreurs sur Amazon sont les suivantes CloudFront.

Rubriques

- Le serveur Origin renvoie l'erreur 500 à CloudFront

Le serveur Origin renvoie l'erreur 500 à CloudFront

Votre serveur d'origine renvoie peut-être une erreur 500 à CloudFront. Pour plus d'informations, consultez les rubriques de dépannage suivantes :

- Si Amazon S3 renvoie une erreur 500, consultez Comment résoudre une erreur HTTP 500 ou 503 provenant d'Amazon S3 ?
- Si API Gateway renvoie une erreur 500, consultez Comment résoudre les erreurs 5xx pour l'API REST d'API Gateway ?.
- Si Elastic Load Balancing renvoie une erreur 500, consultez HTTP 500 : erreur de serveur interne dans le Guide de l'utilisateur des Application Load Balancers.

Si la liste précédente ne résout pas l'erreur 500, le problème est peut-être dû au fait qu'un CloudFront point de présence renvoie une erreur interne au serveur. Vous pouvez également contacter Support pour obtenir de l'aide.

Code d'état HTTP 502 (Passerelle incorrecte)

CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) lorsqu'il CloudFront n'a pas pu servir l'objet demandé car il n'a pas pu se connecter au serveur d'origine.

Si vous utilisez Lambda@Edge, le problème peut être lié à une erreur de validation Lambda. Si vous recevez une erreur HTTP 502 avec le code `NonS3OriginDnsError` d'erreur, il est probable qu'un problème de configuration DNS CloudFront empêche la connexion à l'origine.

Rubriques

- SSL/TLS échec de négociation entre CloudFront et un serveur d'origine personnalisé
- Origin ne répond pas avec « pris en charge » ciphers/protocols
- SSL/TLS le certificat d'origine est expiré, non valide, auto-signé ou la chaîne de certificats n'est pas dans le bon ordre
- L'origine ne répond pas sur des ports spécifiés dans les paramètres de l'origine
- Erreur de validation Lambda
- CloudFront erreur de validation de fonction
- Erreur DNS (NonS3OriginDnsError)
- Erreur 502 pour une origine Application Load Balancer

- Erreur 502 pour une origine API Gateway

SSL/TLS échec de négociation entre CloudFront et un serveur d'origine personnalisé

Si vous utilisez une origine personnalisée qui nécessite le protocole HTTPS entre CloudFront et votre origine, des noms de domaine incompatibles peuvent provoquer des erreurs. Le SSL/TLS certificat de votre origine doit inclure un nom de domaine qui correspond soit au domaine d'origine que vous avez spécifié pour la CloudFront distribution, soit à l'`Host`en-tête de la demande d'origine.

Si les noms de domaine ne correspondent pas, l' SSL/TLS établissement de liaison échoue et CloudFront renvoie un code d'état HTTP 502 (Bad Gateway) et définit l'`X-Cache`en-tête sur. `Error from cloudfront`

Pour déterminer si des noms de domaine du certificat correspondent au Domaine de l'origine dans la distribution ou l'en-tête `Host`, vous pouvez utiliser un outil de vérification SSL en ligne ou OpenSSL. Si les noms de domaine ne correspondent pas, vous avez deux options :

- Obtenez un nouveau SSL/TLS certificat qui inclut les noms de domaine applicables.

  Si vous utilisez AWS Certificate Manager (ACM), consultez la section Demande de certificat public dans le Guide de AWS Certificate Manager l'utilisateur pour demander un nouveau certificat.
- Modifiez la configuration de distribution afin de CloudFront ne plus essayer d'utiliser le protocole SSL pour vous connecter à votre origine.

Outil de vérification SSL en ligne

Pour trouver un outil de test SSL, recherchez sur Internet « online ssl checker ». Généralement, vous spécifiez le nom de votre domaine et l'outil renvoie diverses informations concernant votre SSL/TLS certificat. Vérifiez que le certificat contient votre nom de domaine dans les champs Common Names ou Subject Alternative Names.

OpenSSL

Pour résoudre les erreurs HTTP 502 provenant de CloudFront, vous pouvez utiliser OpenSSL pour essayer d'établir une SSL/TLS connexion avec votre serveur d'origine. Si OpenSSL ne parvient pas à établir une connexion, cela peut indiquer un problème avec la configuration de votre serveur d'SSL/TLS origine. Si OpenSSL est en mesure d'établir une connexion, il renvoie des informations sur le certificat du serveur d'origine, y compris le nom commun (champ `Subject CN`) et le nom alternatif d'objet (champ `Subject Alternative Name`) du certificat.

Utilisez la commande OpenSSL suivante pour tester la connexion à votre serveur d'origine (remplacez-la par le nom *origin domain* de domaine de votre serveur d'origine, tel que example.com) :

```
openssl s_client -connect origin domain name:443
```

Si les conditions suivantes sont réunies :

- Votre serveur d'origine prend en charge plusieurs noms de domaine avec plusieurs SSL/TLS certificats
- Votre distribution est configurée pour transférer l'en-tête `Host` vers l'origine

Ajoutez ensuite l'`-servername`option à la commande OpenSSL, comme dans l'exemple suivant (remplacez *CNAME* par le CNAME configuré dans votre distribution) :

```
openssl s_client -connect origin domain name:443 -servername CNAME
```

Origin ne répond pas avec « pris en charge » ciphers/protocols

CloudFront se connecte aux serveurs d'origine à l'aide de chiffrements et de protocoles. Pour obtenir la liste des chiffrements et des protocoles pris CloudFront en charge, consultez. the section called "Protocoles et chiffrements pris en charge entre CloudFront et l'origine" Si votre origine ne répond pas avec l'un de ces chiffrements ou protocoles dans l'SSL/TLS échange, la connexion CloudFront échoue. Vous pouvez vérifier que votre origine prend en charge les chiffrements et les protocoles à l'aide d'un outil en ligne tel que SSL Labs. Saisissez le nom de domaine de votre origine dans le champ Hostname, puis choisissez Submit. Consultez les champs Noms Communs et autres noms (SAN) du test pour savoir si ces noms correspondent au nom de domaine de votre origine. A la fin du test, consultez les sections Protocols et Cipher Suites des résultats pour connaître les chiffrements ou les protocoles pris en charge par votre origine. Comparez-les à la liste des the section called "Protocoles et chiffrements pris en charge entre CloudFront et l'origine".

SSL/TLS le certificat d'origine est expiré, non valide, auto-signé ou la chaîne de certificats n'est pas dans le bon ordre

Si le serveur d'origine renvoie les informations suivantes, CloudFront interrompt la connexion TCP, renvoie le code d'état HTTP 502 (Bad Gateway) et définit l'`X-Cache`en-tête sur : `Error from cloudfront`

- Certificat expiré

- Certificat non valide
- Self-signed certificat
- Chaîne de certificats dans le désordre

> **Note**
>
> Si la chaîne complète de certificats, y compris le certificat intermédiaire, n'est pas présente, la connexion TCP est CloudFront interrompue.

Pour plus d'informations sur l'installation d'un SSL/TLS certificat sur votre serveur d'origine personnalisé, consultezthe section called “Exigence du protocole HTTPS vers une origine personnalisée”.

L’origine ne répond pas sur des ports spécifiés dans les paramètres de l’origine

Lorsque vous créez une origine sur votre CloudFront distribution, vous pouvez définir les ports qui CloudFront se connectent à l'origine pour le trafic HTTP et HTTPS. Par défaut, il s'agit du protocole TCP 80/443. Vous avez la possibilité de modifier ces ports. Si votre origine rejette le trafic sur ces ports pour une raison quelconque, ou si votre serveur principal ne répond pas sur les ports, la connexion CloudFront échouera.

Pour résoudre ces problèmes, vérifiez les pare-feu qui s’exécutent dans votre infrastructure et vérifiez qu’ils ne bloquent pas les plages IP prises en charge. Pour plus d’informations, consultez Plages d’adresses IP AWS dans le Guide de l’utilisateur Amazon VPC. Vous pouvez également vérifier que votre serveur web s’exécute sur l’origine.

Erreur de validation Lambda

Si vous utilisez Lambda@Edge, un code de statut HTTP 502 peut indiquer que la réponse de votre fonction Lambda était mal formulée ou comprenait du contenu non valide. Pour plus d’informations sur le dépannage des erreurs Lambda@Edge, consultez Test et débogage des fonctions Lambda@Edge.

CloudFront erreur de validation de fonction

Si vous utilisez des CloudFront fonctions, un code d'état HTTP 502 peut indiquer que la CloudFront fonction essaie d'ajouter, de supprimer ou de modifier un en-tête en lecture seule. Cette erreur ne s’affiche pas pendant le test, mais elle apparaîtra une fois que vous aurez déployé la fonction et

exécuté la demande. Pour résoudre cette erreur, vérifiez et mettez à jour votre CloudFront fonction. Pour plus d'informations, consultez Mise à jour de fonctions.

Erreur DNS (**`NonS3OriginDnsError`**)

Une erreur HTTP 502 avec le code `NonS3OriginDnsError` d'erreur indique qu'un problème de configuration DNS CloudFront empêche la connexion à l'origine. Si vous obtenez cette erreur CloudFront, assurez-vous que la configuration DNS de l'origine est correcte et qu'elle fonctionne.

Lorsqu'il CloudFront reçoit une demande pour un objet qui a expiré ou qui n'est pas dans son cache, il adresse une demande à l'origine pour obtenir l'objet. Pour envoyer une requête à l'origine avec succès, CloudFront exécute une résolution DNS sur le domaine d'origine. Si le service DNS de votre domaine rencontre des problèmes, CloudFront impossible de résoudre le nom de domaine pour obtenir l'adresse IP, ce qui entraîne une erreur HTTP 502 (`NonS3OriginDnsError`). Pour résoudre ce problème, contactez votre fournisseur DNS ou, si vous utilisez Amazon Route 53, consultez Pourquoi est-ce que je ne peux pas accéder à mon site Web qui utilise les services DNS Route 53 ?

Pour résoudre davantage ce problème, assurez-vous que les serveurs de noms faisant autorité du domaine racine ou de la zone apex de votre origine (par exemple`example.com`) fonctionnent correctement. Vous pouvez utiliser les commandes suivantes pour trouver les serveurs de noms pour votre origine apex, à l'aide d'un outil tel que dig ou nslookup :

```
dig OriginAPEXDomainName NS +short
```

```
nslookup -query=NS OriginAPEXDomainName
```

Quand vous avez les noms de vos serveurs de noms, utilisez les commandes suivantes pour interroger le nom de domaine de votre origine sur ceux-ci afin de vous assurer qu'ils répondent :

```
dig OriginDomainName @NameServer
```

```
nslookup OriginDomainName NameServer
```

> **Important**
>
> Assurez-vous d'effectuer ce dépannage DNS à l'aide d'un ordinateur connecté à Internet public. CloudFront résout le domaine d'origine à l'aide du DNS public sur Internet. Il est donc important de résoudre les problèmes dans un contexte similaire.

Si votre origine est un sous-domaine dont l'autorité DNS est déléguée à un serveur de noms différent du domaine racine, assurez-vous que les enregistrements du serveur de noms (NS) et du début de l'autorité (SOA) sont correctement configurés pour le sous-domaine. Vous pouvez vérifier ces enregistrements à l'aide de commandes similaires aux exemples précédents.

Pour plus d'informations sur DNS, consultez les Concepts du système de noms de domaine (DNS) dans la documentation d'Amazon Route 53.

Erreur 502 pour une origine Application Load Balancer

Si vous utilisez Application Load Balancer comme origine et que vous recevez une erreur 502, consultez Comment résoudre les erreurs HTTP 502 d'Application Load Balancer ?.

Erreur 502 pour une origine API Gateway

Si vous utilisez API Gateway et que vous recevez une erreur 502, consultez Comment résoudre les erreurs HTTP 502 provenant des API REST d'API Gateway utilisant une intégration de proxy Lambda ?.

Code d'état HTTP 503 (Service non disponible)

Un code de statut HTTP 503 (Service non disponible) indique généralement un problème de performance sur le serveur d'origine. Dans de rares cas, cela indique qu'il est CloudFront temporairement impossible de répondre à une demande en raison de contraintes de ressources à un emplacement périphérique.

Si vous utilisez Lambda @Edge ou CloudFront Functions, le problème peut être une erreur d'exécution ou une erreur de dépassement de limite Lambda @Edge.

Si vous utilisez le protocole TLS mutuel d'origine (mTLS d'origine), le problème peut être dû à des tentatives infructueuses répétées d'établissement d'une connexion avec un certificat spécifique.

Rubriques

- Le serveur d'origine n'a pas suffisamment de capacité pour prendre en charge le débit de requêtes
- CloudFront a provoqué l'erreur en raison de contraintes de ressources à l'emplacement périphérique
- CloudFront a provoqué l'erreur pour une origine configurée avec un TLS mutuel
- Erreur d'exécution de Lambda @Edge ou CloudFront de fonction
- Dépassement d'une limite Lambda@Edge

Le serveur d’origine n’a pas suffisamment de capacité pour prendre en charge le débit de requêtes

Lorsqu'un serveur d'origine n'est pas disponible ou n'est pas en mesure de traiter les demandes entrantes, il renvoie un code d'état HTTP 503 (Service non disponible). CloudFront transmet ensuite l'erreur à l'utilisateur. Pour résoudre ce problème, essayez les solutions suivantes :

- Si vous utilisez Amazon S3 comme serveur d’origine :
  - Vous pouvez envoyer 3 500 PUT/COPY/POST/DELETE ou 5 500 GET/HEAD demandes par seconde par préfixe Amazon S3 partitionné. Lorsque Amazon S3 renvoie une réponse 503 Ralentissement, cela indique généralement un taux de demandes trop élevé sur un préfixe Amazon S3 donné.

    Étant donné que les taux de demandes s’appliquent par préfixe dans un compartiment S3, les objets doivent être répartis entre plusieurs préfixes. À mesure que le taux de demandes sur les préfixes augmente progressivement, Amazon S3 augmente verticalement afin de traiter les demandes de chaque préfixe séparément. Par conséquent, le taux global de demandes que le compartiment peut traiter est un multiple du nombre de préfixes.
  - Pour plus d’informations, consultez Optimisation de la performance d’Amazon S3 dans le Guide de l’utilisateur Amazon Simple Storage Service.
- Si vous utilisez Elastic Load Balancing comme serveur d’origine :
  - Assurez-vous que vos instances dorsales peuvent répondre à la surveillance de l’état.
  - Assurez-vous que votre équilibreur de charge et vos instances dorsales peuvent gérer la charge.

  Pour plus d’informations, consultez :
  - Comment résoudre les erreurs 503 renvoyées lors de l’utilisation de Classic Load Balancer ?
  - Comment résoudre les erreurs 503 (service non disponible) depuis mon Application Load Balancer ?
- Si vous utilisez une origine personnalisée :
  - Examinez les journaux des applications pour vous assurer que votre origine dispose de ressources suffisantes, telles que la mémoire, le processeur et la taille du disque.
  - Si vous utilisez Amazon EC2 comme système dorsal, assurez-vous que le type d’instance dispose des ressources appropriées pour traiter les demandes entrantes. Pour plus d’informations, consultez Types d’instances dans le Guide de l’utilisateur Amazon EC2.
- Si vous utilisez API Gateway :

- Cette erreur est liée à l'intégration dorsale lorsque l'API API Gateway n'est pas en mesure de recevoir une réponse. Le serveur dorsal peut être :
  - Surchargé au-delà de sa capacité et incapable de traiter les nouvelles demandes des clients.
  - En maintenance temporaire.
- Pour résoudre cette erreur, consultez les journaux de votre application API Gateway afin de déterminer s'il existe un problème de capacité du système dorsal, d'intégration ou autre.

CloudFront a provoqué l'erreur en raison de contraintes de ressources à l'emplacement périphérique

Vous recevrez cette erreur dans les rares cas où vous ne CloudFront pouvez pas acheminer les demandes vers le meilleur emplacement périphérique disponible suivant et ne pouvez donc pas répondre à une demande. Cette erreur est courante lorsque vous effectuez des tests de charge sur votre distribution CloudFront. Pour essayer d'éviter ceci, suivez les conseils de the section called "Test de charge CloudFront" pour éviter les erreurs 503 (dépassement de capacité).

Si cela se produit dans votre environnement de production, contactez Support.

CloudFront a provoqué l'erreur pour une origine configurée avec un TLS mutuel

Si votre distribution utilise le protocole TLS mutuel (mTLS) pour se connecter à une origine personnalisée, elle CloudFront peut renvoyer un code d'état HTTP 503 lorsqu'elle ne parvient pas à établir de connexions avec l'origine. Cela peut se produire lorsque l'origine ne parvient pas à effectuer les handshakes TLS à plusieurs reprises ou qu'elle est inaccessible en raison de problèmes de DNS ou de connectivité. Cette condition est temporaire : le trafic normal reprend CloudFront automatiquement une fois que l'origine est à nouveau accessible.

Pour résoudre ce problème :

- Vérifiez que le certificat client approprié est associé à votre distribution et qu'il n'a pas expiré. Si vous avez récemment mis à jour le certificat, attendez que la modification se propage avant qu'elle ne prenne effet.
- Vérifiez que l'origine est accessible et que les enregistrements DNS sont résolus correctement.

Si le problème persiste malgré la configuration du certificat approprié dans votre environnement de production, contactez Support.

Erreur d'exécution de Lambda @Edge ou CloudFront de fonction

Si vous utilisez Lambda @Edge ou CloudFront Functions, un code d'état HTTP 503 peut indiquer que votre fonction a renvoyé une erreur d'exécution.

Pour plus d'informations sur l'identification et la résolution des erreurs Lambda@Edge, consultez Test et débogage des fonctions Lambda@Edge.

Pour plus d'informations sur les CloudFront fonctions de test, consultezFonctions de test.

Dépassement d'une limite Lambda@Edge

Si vous utilisez Lambda@Edge, un code d'état HTTP 503 peut indiquer que Lambda a renvoyé une erreur. Cette erreur peut être due à l'une des raisons suivantes :

- Le nombre d'exécutions de fonctions a dépassé l'un des quotas définis par Lambda pour limiter les exécutions dans un Région AWS (exécutions simultanées ou fréquence d'appel).
- La fonction a dépassé le quota d'expiration de la fonction Lambda.

Pour plus d'informations sur les quotas Lambda@Edge, consultez Quotas sur Lambda@Edge. Pour plus d'informations sur l'identification et la résolution des erreurs Lambda@Edge, consultez the section called "Test et débogage". Vous pouvez également consulter les Quotas de service Lambda dans le Guide du développeur AWS Lambda .

Code d'état HTTP 504 (Délai d'attente de passerelle expiré)

Un code d'état HTTP 504 (délai d'expiration de la passerelle) indique que lors du CloudFront transfert d'une demande vers l'origine (car l'objet demandé ne se trouvait pas dans le cache périphérique), l'une des situations suivantes s'est produite :

- L'origine a renvoyé un code d'état HTTP 504 à CloudFront.
- L'origine n'a pas répondu avant l'expiration de la demande.

CloudFront renverra un code d'état HTTP 504 si le trafic est bloqué vers l'origine par un pare-feu ou un groupe de sécurité, ou si l'origine n'est pas accessible sur Internet. Commencez par vérifier ces problèmes. Ensuite, si l'accès n'est pas le problème, explorez les retards de l'application et les délais d'attente du serveur pour mieux identifier et résoudre les problèmes.

Rubriques

- Configurez le pare-feu de votre serveur d'origine pour autoriser CloudFront le trafic
- Configurez les groupes de sécurité sur votre serveur d'origine pour autoriser CloudFront le trafic
- Rendez accessible votre serveur d’origine personnalisée sur Internet
- Recherchez et corrigez des réponses retardées à partir des applications sur votre serveur d’origine

Configurez le pare-feu de votre serveur d'origine pour autoriser CloudFront le trafic

Si le pare-feu de votre serveur d'origine bloque le CloudFront trafic et CloudFront renvoie un code d'état HTTP 504, il est donc conseillé de vous assurer que ce n'est pas le problème avant de vérifier s'il y a d'autres problèmes.

La méthode que vous utilisez pour déterminer s’il s’agit d’un problème avec votre pare-feu dépend du système que votre serveur d’origine utilise :

- Si vous utilisez un pare-feu IPTables sur un serveur Linux, vous pouvez rechercher des outils et des informations qui vous aideront à travailler avec IPTables.
- Si vous utilisez le pare-feu de Windows sur un serveur Windows, consultez Ajouter ou modifier la règle de pare-feu dans la documentation Microsoft.

Lorsque vous évaluez la configuration du pare-feu sur votre serveur d'origine, recherchez les pare-feux ou les règles de sécurité qui bloquent le trafic en provenance d'emplacements CloudFront périphériques, en fonction de la plage d'adresses IP publiée. Pour plus d’informations, consultez Emplacements et plages d'adresses IP des serveurs CloudFront Edge.

Si la plage d'adresses CloudFront IP est autorisée à se connecter à votre serveur d'origine, veillez à mettre à jour les règles de sécurité de votre serveur pour intégrer les modifications. Vous pouvez vous abonner à une rubrique Amazon SNS et recevoir des notifications lorsque le fichier de plage d’adresses IP est mis à jour. Après avoir reçu la notification, vous pouvez utiliser le code pour extraire le fichier, l’analyser et effectuer des ajustements pour votre environnement local. Pour plus d'informations, consultez la section S'abonner aux modifications d'adresses IP AWS publiques en utilisant Amazon SNS sur le blog d' AWS actualités.

Configurez les groupes de sécurité sur votre serveur d'origine pour autoriser CloudFront le trafic

Si votre origine utilise Elastic Load Balancing, passez en revue les groupes de sécurité ELB et assurez-vous qu'ils autorisent le trafic entrant. CloudFront

Vous pouvez également l'utiliser AWS Lambda pour mettre à jour automatiquement vos groupes de sécurité afin d'autoriser le trafic entrant en provenance de CloudFront.

Rendez accessible votre serveur d’origine personnalisée sur Internet

Si vous ne CloudFront pouvez pas accéder à votre serveur d'origine personnalisé parce qu'il n'est pas accessible au public sur Internet, CloudFront renvoie une erreur HTTP 504.

CloudFront les sites périphériques se connectent aux serveurs d'origine via Internet. Si votre origine personnalisée se trouve sur un réseau privé, CloudFront impossible de l'atteindre. Pour cette raison, vous ne pouvez pas utiliser de serveurs privés, y compris des équilibreurs de charge classiques internes, comme serveurs d' CloudFrontorigine.

Pour vérifier que le trafic Internet peut se connecter à votre serveur d'origine, exécutez les commandes suivantes (où se *OriginDomainName* trouve le nom de domaine de votre serveur) :

Pour le trafic HTTPS :

- NC -ZV 443 *OriginDomainName*
- telnet 443 *OriginDomainName*

Pour le trafic HTTP :

- NC -ZV 80 *OriginDomainName*
- telnet 80 *OriginDomainName*

Recherchez et corrigez des réponses retardées à partir des applications sur votre serveur d’origine

Les délais d’attente du serveur sont souvent le résultat d’une application qui met beaucoup de temps à répondre ou de la définition d’une valeur de délai d’attente trop faible.

Une solution rapide pour essayer d'éviter des erreurs HTTP 504 consiste à définir simplement une valeur de délai d'attente CloudFront plus élevée pour votre distribution. Cependant, nous vous recommandons de commencer par vous assurer que vous traitez tous les problèmes de performances et de latence liés à l’application et au serveur d’origine. Ensuite, vous pouvez définir une valeur de délai d’attente raisonnable qui vise à empêcher les erreurs HTTP 504 et qui offre une bonne réactivité aux utilisateurs.

Voici une vue d'ensemble des étapes que vous pouvez suivre pour rechercher des problèmes de performances et les corriger :

1. Mesurez la latence standard et à charge élevée (réactivité) de votre application web.
2. Ajoutez d'autres ressources, telles que l'UC ou la mémoire, si nécessaire. Prenez d'autres mesures pour résoudre les problèmes, telles que le réglage des requêtes de base de données pour prendre en charge les scénarios à charge élevée.
3. Si nécessaire, ajustez la valeur du délai d'attente pour votre CloudFront distribution.

Vous trouverez ci-après des détails relatifs à chaque étape.

Mesure de la latence standard et à charge élevée

Pour déterminer si un ou plusieurs serveurs d'application web dorsaux présentent une latence élevée, exécutez la commande curl Linux suivante sur chaque serveur :

```
curl -w "DNS Lookup Time: %{time_namelookup} \nConnect time: %{time_connect}
 \nTLS Setup: %{time_appconnect} \nRedirect Time: %{time_redirect} \nTime to first
 byte: %{time_starttransfer} \nTotal time: %{time_total} \n" -o /dev/null https://
www.example.com/yourobject
```

> **Note**
>
> Si vous exécutez Windows sur vos serveurs, vous pouvez rechercher et télécharger curl pour Windows afin d'exécuter une commande similaire.

Lorsque vous mesurez et évaluez la latence d'une application qui s'exécute sur votre serveur, gardez à l'esprit les points suivants :

- Les valeurs de latence sont relatives à chaque application. Toutefois, un délai jusqu'au premier octet en millisecondes plutôt qu'en secondes ou plus est raisonnable.
- Si vous mesurez la latence de l'application sous une charge normale et qu'elle est satisfaisante, sachez que les utilisateurs peuvent tout de même connaître des dépassements de délais d'attente sous une charge élevée. Lorsqu'il y a une forte demande, les serveurs peuvent avoir des réponses différées ou aucune réponse du tout. Pour essayer d'éviter les problèmes de latence en cas de charge élevée, vérifiez les ressources de vos serveurs telles que l'UC, la mémoire et les lectures

et écritures sur disque pour vous assurer que vos serveurs ont la capacité d'évoluer suffisamment pour traiter une charge élevée.

Vous pouvez exécuter la commande Linux suivante pour vérifier la mémoire utilisée par les processus Apache :

```
watch -n 1 "echo -n 'Apache Processes: ' && ps -C apache2 --no-headers | wc -l && free -m"
```

- Une utilisation intensive de l'UC sur le serveur peut réduire considérablement les performances d'une application. Si vous utilisez une instance Amazon EC2 pour votre serveur principal, consultez les CloudWatch statistiques du serveur afin de vérifier l'utilisation du processeur. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon. Ou, si vous utilisez votre propre serveur, reportez-vous à la documentation d'aide du serveur pour obtenir des instructions sur la manière de vérifier l'utilisation de l'UC.
- Recherchez d'autres problèmes potentiels sous des charges élevées, telles que les requêtes de base de données qui s'exécutent lentement dans le cas d'un grand volume de demandes.

Ajout de ressources et réglage des serveurs et des bases de données

Une fois que vous avez évalué la réactivité de vos applications et serveurs, assurez-vous d'avoir les ressources suffisantes en place pour gérer des situations à trafic standard et à charge élevée :

- Si vous possédez votre propre serveur, assurez-vous qu'il a suffisamment d'UC, de mémoire et d'espace disque pour gérer les demandes des utilisateurs, en fonction de votre évaluation.
- Si vous utilisez une instance Amazon EC2 comme serveur dorsal, assurez-vous que le type d'instance dispose des ressources appropriées pour traiter les demandes entrantes. Pour plus d'informations, consultez Types d'instances dans le Guide de l'utilisateur Amazon EC2.

En outre, prenez en compte les étapes de réglage suivantes pour essayer d'éviter le dépassement des délais d'attente :

- Si la valeur du délai jusqu'au premier octet qui est renvoyée par la commande curl semble élevée, prenez des mesures pour améliorer les performances de votre application. L'amélioration de la réactivité de l'application aidera à son tour à réduire les erreurs de dépassement de délai.
- Réglez les requêtes de base de données pour vous assurer que de grands volumes de requêtes peuvent être gérés sans ralentir les performances.

- Configurez des connexions keep-alive (persistantes) sur votre serveur dorsal. Cette option permet d'éviter les latences qui se produisent lorsque les connexions doivent être rétablies pour des demandes ou des utilisateurs suivants.
- Si vous utilisez Elastic Load Balancing comme origine, les causes possibles d'une erreur 504 sont les suivantes :
  - L'équilibreur de charge n'a pas réussi à établir une connexion vers la cible avant l'expiration du délai de connexion (10 secondes).
  - L'équilibreur de charge à établi une connexion vers la cible mais la cible n'a pas répondu avant la fin du délai d'inactivité.
  - La liste de contrôle d'accès (ACL) réseau pour le sous-réseau n'a pas autorisé le trafic depuis les cibles vers les nœuds d'équilibreur de charge sur les ports éphémères (1024-65535).
  - La cible a renvoyé un en-tête Content-length plus grand que le corps de l'entité. L'équilibreur de charge a expiré en attendant les octets manquants.
  - La cible est une fonction Lambda et Lambda n'a pas répondu avant l'expiration du délai de connexion.

  Pour plus d'informations sur la réduction de la latence, consultez Comment résoudre les problèmes de latence élevée sur mon ELB Classic Load Balancer ?
- Si vous utilisez MediaTailor comme origine, les causes possibles d'une erreur 504 sont les suivantes :
  - Si les URL relatives sont mal gérées, les MediaTailor joueurs peuvent recevoir des URL mal formées.
  - Si MediaPackage est l'origine du manifeste pour MediaTailor MediaPackage 404 erreurs de manifeste peuvent MediaTailor entraîner le renvoi d'une erreur 504.
  - L'exécution de la demande au serveur d' MediaTailor origine prend plus de 2 secondes.
- Si vous utilisez Amazon API Gateway comme origine, les causes possibles d'une erreur 504 sont les suivantes :
  - Une demande d'intégration dépasse le délai maximal d'intégration défini pour votre API REST API Gateway. Pour plus d'informations, consultez Comment résoudre les erreurs de délai dépassé API HTTP 504 avec API Gateway ?

Si nécessaire, ajustez la valeur du CloudFront délai d'attente

Vous avez peut-être évalué et résolu la lenteur des performances des applications, la capacité du serveur d'origine et d'autres problèmes, mais les utilisateurs rencontrent toujours des erreurs HTTP

504. Dans ce cas, pensez à modifier l'heure spécifiée dans votre distribution pour le délai de réponse d'origine. Pour plus d'informations, consultez the section called “Délai de réponse”.

Test de charge CloudFront

Les méthodes de test de charge traditionnelles ne fonctionnent pas bien avec CloudFront car CloudFront utilise le DNS pour équilibrer les charges entre des emplacements périphériques géographiquement dispersés et au sein de chaque emplacement périphérique. Lorsqu'un client demande du contenu à CloudFront, il reçoit une réponse DNS qui inclut un ensemble d'adresses IP. Si vous effectuez un test en envoyant des requêtes à une seule des adresses IP renvoyées par le DNS, vous testez uniquement un petit sous-ensemble de ressources dans un emplacement CloudFront périphérique, ce qui ne représente pas exactement les modèles de trafic réels. En fonction du volume de données demandé, les tests effectués de cette manière peuvent surcharger et dégrader les performances de ce petit sous-ensemble de CloudFront serveurs.

CloudFront est conçu pour s'adapter aux utilisateurs qui ont différentes adresses IP de clients et différents résolveurs DNS dans plusieurs régions géographiques. Pour effectuer des tests de charge qui évaluent avec précision les CloudFront performances, nous vous recommandons d'effectuer toutes les opérations suivantes :

- Envoyez les demandes des clients depuis plusieurs régions géographiques.
- Configurez votre test de manière à ce que chaque client effectue une demande DNS indépendante. Chaque client reçoit alors de DNS un ensemble différent d'adresses IP.
- Pour chaque client qui effectue des demandes, répartissez ces dernières sur l'ensemble des adresses IP renvoyées par le DNS. Cela garantit que la charge est répartie sur plusieurs serveurs situés en CloudFront périphérie.

Remarques

- Les tests de charge ne sont pas autorisés sur les comportements de cache dotés de déclencheurs de demandes ou de réponses d'utilisateurs Lambda@Edge.
- Les tests de charge ne sont pas autorisés sur les origines sur lesquelles Origin Shield est activé.

Quotas

Vous pouvez demander une augmentation de CloudFront quota en utilisant les options suivantes :

- Vous pouvez utiliser la console Service Quotas ou l' AWS Command Line Interface. Pour plus d'informations, consultez les rubriques suivantes :
  - Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas
  - request-service-quota-increase dans la référence de commande AWS CLI
- Si aucun CloudFront quota n'est disponible dans Service Quotas, utilisez le AWS Support Center Console pour créer un cas d'augmentation du quota de service.

CloudFront est soumis aux quotas suivants.

Rubriques

- Quotas généraux
- Quotas généraux sur les distributions
- Quotas généraux sur les politiques
- Quotas sur les MTL et les trust stores
- Quotas relatifs aux CloudFront fonctions
- Quotas relatifs aux fonctions de connexion
- Quotas sur les magasins de clés-valeurs
- Quotas sur Lambda@Edge
- Quotas sur les certificats SSL
- Quotas sur les invalidations
- Quotas sur les groupes clés
- Quotas sur WebSocket les connexions
- Quotas sur le chiffrement au niveau du champ
- Quotas sur les cookies (paramètres de cache hérités)
- Quotas sur les chaînes de requêtes (paramètres de cache hérités)
- Quotas sur les en-têtes
- Quotas sur les distributions multi-locataires
- Informations connexes

Quotas généraux

Entité	Quota par défaut
Débit de transfert des données par distribution (Ce quota ne s'applique pas aux distributions souscrites à des plans tarifaires CloudFront forfaitaires. Pour plus d'informations, voir???.)	150 Gb/s Demander une augmentation du quota
Demandes par seconde par distribution (Ce quota ne s'applique pas aux distributions souscrites à des plans tarifaires CloudFront forfaitaires. Pour plus d'informations, voir???.)	250 000 Demander une augmentation du quota
Balises pouvant être ajoutées à une distribution	50 Demander une augmentation du quota
Fichiers que vous pouvez servir par distribution	Pas de quota
Longueur maximale d’une demande ou d’une réponse de l’origine, en incluant les en-têtes et les chaînes de requête, mais en excluant le contenu du corps	32 768 octets
Longueur maximale d'une URL	8 192 octets
Nombre maximum de configurations de livraison de journaux d'accès en temps réel par Compte AWS	150
Nombre maximum d'associations par ACL Web	100 Demander une augmentation du quota

Quotas généraux sur les distributions

Entité	Quota par défaut
Noms de domaine alternatifs (CNAME) par distribution Pour plus d'informations, consultez Utilisation d'URL personnalisées en ajoutant des noms de domaine alternatifs (CNAME).	100 Demander une augmentation du quota
Comportements de cache par distribution	75 Demander une augmentation du quota
Tentatives de connexion par origine Pour plus d'informations, consultez Tentatives de connexion.	1 à 3
Délai de connexion par origine Pour plus d'informations, consultez Délai de connexion.	1 à 10 secondes
Délai de réponse par origine Ceci est également appelé délai d'attente de la lecture d'origine ou délai d'attente de la demande d'origine. Pour plus d'informations, consultez Délai de réponse.	1 à 120 secondes Demander une augmentation du quota
Keep-alive délai d'expiration par origine Pour plus d'informations, consultez Keep-alive délai d'expiration (origines personnalisées et VPC uniquement).	1 à 300 secondes Demander une augmentation du quota
Distributions par Compte AWS Pour plus d'informations, consultez Créer une distribution.	500

Entité	Quota par défaut
	Demander une augmentation du quota
Distributions par contrôle d’accès d’origine	100 Demander une augmentation du quota
Distributions au sein de la chaîne de demandes adressées au point de terminaison d’origine Il n’est pas recommandé de mettre une distribution devant une autre distribution. Le dépassement de ce quota entraîne une erreur 403.	2
Compression de fichiers : plage de tailles de fichiers qui CloudFront compresse Pour plus d’informations, consultez Diffusion de fichiers compressés.	1 000 à 10 000 000 octets
Taille de fichier maximale pouvant être mise en cache par réponse HTTP GET. Seules les réponses pour HTTP GET sont mises en cache. Les réponses pour POST et PUT ne sont pas mises en cache.	50 Go
Taille maximale du corps d'une requête HTTP.	64 Go
Contrôles d'accès à Origin par Compte AWS	100 Demander une augmentation du quota

Entité	Quota par défaut
Identités d'accès à l'origine par Compte AWS	100 Demander une augmentation du quota
Origines par distribution	100 Demander une augmentation du quota
Groupes d'origine par distribution	10 Demander une augmentation du quota
Répartition des distributions par Compte AWS Pour plus d’informations, consultez the section called “Utilisation du déploiement continu pour tester en toute sécurité les changements”.	20 Demander une augmentation du quota
Distributions associées à la même origine VPC	50
Origines du VPC par Compte AWS	25 Demander une augmentation du quota
Nombre maximal de distributions qui peuvent être associées à une seule liste d’adresses IP statiques en unidiffusion.	100 Demander une augmentation du quota

Quotas généraux sur les politiques

Entité	Quota par défaut
Politiques de cache personnalisées par Compte AWS (Ne s'applique pas aux politiques de cache CloudFront gérées)	20 Demander une augmentation du quota
Distributions associées à la même politique de cache	100
Chaînes de requête par politique de cache	10 Demander une augmentation du quota
En-têtes par politique de cache	10 Demander une augmentation du quota
Cookies par politique de cache	10 Demander une augmentation du quota
Longueur totale combinée de tous les noms de chaîne de requête, d'en-tête et de cookie dans une politique de cache	1 024
Politiques de demande d'origine personnalisées par Compte AWS (Ne s'applique pas aux politiques de CloudFront gestion des demandes d'origine)	20 Demander une augmentation du quota
Distributions associées à la même politique de demande d'origine	100

Entité	Quota par défaut
Chaînes de requête par politique de demande d'origine	10 Demander une augmentation du quota
En-têtes par politique de demande d'origine	10 Demander une augmentation du quota
Politique de demande de cookies par origine	10 Demander une augmentation du quota
Longueur totale combinée de tous les noms de chaîne de requête, d'en-tête et de cookie dans une stratégie de demande d'origine	1 024
Politiques d'en-têtes de réponse personnalisées par Compte AWS (Ne s'applique pas aux politiques relatives aux en-têtes de réponse CloudFront gérés)	20 Demander une augmentation du quota
Distributions associées à la même politique d’en-têtes de réponses	100 Demander une augmentation du quota
En-têtes personnalisés par politique d’en-têtes de réponses	10 Demander une augmentation du quota

Entité	Quota par défaut
Politiques de déploiement continu par Compte AWS	20 Demander une augmentation du quota

Quotas sur les MTL et les trust stores

Entité	Quota par défaut
Trust Stores par Compte AWS	20 Demander une augmentation du quota
Distributions par magasin de confiance	300
Taille du bundle CA	1 Mo
Taille du certificat dans le bundle CA	16384 Demander une augmentation du quota
Nombre de certificats dans le bundle CA	25
Profondeur de la chaîne de certificats	4

Quotas relatifs aux CloudFront fonctions

Entité	Quota par défaut
Fonctions par Compte AWS	100

Entité	Quota par défaut
Taille de fonction maximale Il ne s'agit pas d'un quota ajustable. Pour stocker des données supplémentaires pour vos CloudFront fonctions, créez un magasin clé-valeur et ajoutez vos paires clé-valeur. Pour plus d'informations, consultez Amazon CloudFront KeyValueStore.	10 Ko
Mémoire de fonction maximale	2 Mo
Distributions associées à la même politique de fonction	100

Outre ces quotas, il existe d'autres restrictions lors de l'utilisation de CloudFront Functions. Pour plus d'informations, consultez Restrictions relatives aux CloudFront fonctions.

Quotas relatifs aux fonctions de connexion

Entité	Quota par défaut
Fonctions de connexion par Compte AWS	100
Taille maximale de la fonction de connexion Il ne s'agit pas d'un quota ajustable. Pour stocker des données supplémentaires pour vos fonctions de connexion, créez un magasin clé-valeur et ajoutez vos paires clé-valeur. Pour plus d'informations, consultez Amazon CloudFront KeyValueStore.	10 Ko
Mémoire maximale de la fonction de connexion	2 Mo
Distributions associées à la même fonction de connexion	100

Outre ces quotas, il existe d'autres restrictions lors de l'utilisation des fonctions de connexion. Pour plus d'informations, consultez Associer une fonction CloudFront de connexion.

Quotas sur les magasins de clés-valeurs

Entité	Quota par défaut
Taille maximale d'une clé dans une paire clé-valeur	512 octets
Taille maximale de la valeur dans une paire clé-valeur	1 Ko
Nombre maximal de paires clé-valeur que vous pouvez mettre à jour dans une seule demande d'API	50 clés ou 3 Mo de charge utile, selon la première valeur atteinte
Taille maximale d'un magasin de clés-valeurs individuel	5 Mo
Nombre maximal de fonctions auxquelles un magasin de clés-valeurs unique peut être associé	100
Nombre maximal de magasins de clés-valeurs par fonction	1
Nombre maximal de magasins de clés-valeurs par compte	200 Demander une augmentation du quota

Quotas sur Lambda@Edge

Quotas généraux

Entité	Quota par défaut
Distributions par Compte AWS lesquelles des fonctions Lambda @Edge peuvent être utilisées	500 Demander une augmentation du quota
Fonctions Lambda@Edge par distribution	100

Entité	Quota par défaut
	Demander une augmentation du quota
Exécutions simultanées **Remarques** • AWS Lambda gère les quotas de simultanéité pour Lambda @Edge. Toutes les fonctions Lambda incluses dans la Région AWS partagent ce quota. • Nous vous recommandons de revoir le quota d'exécutions simultanées dans tous les pays d' Régions AWS où vous vous attendez à ce que les requêtes de vos spectateurs provienne nt. En outre, chaque instance de votre fonction Lambda @Edge peut traiter jusqu'à 10 requêtes par seconde. La limite d'invocation totale est de 10 fois votre limite de simultanéité. Pour plus d'informations, consultez les rubriques suivantes du guide du AWS Lambda développeur : • Comprendre la mise à l'échelle des fonctions Lambda • Demandes d'API Lambda	1 000 (dans chaque Région AWS) Demander une augmentation du quota
Distributions associées à la même politique de fonction	500
Taille compressée maximale de votre fonction Lambda et des bibliothè ques associées	50 Mo

Entité	Quota par défaut
Demandes Lambda@Edge par seconde (dans chaque Région AWS prise en charge). Pour plus d'informations, consultez Quotas de simultanéité dans le Guide du développeur AWS Lambda .	10 000
Taille de la mémoire de la fonction	Identique aux quotas Lambda.
Fonction timeout. Cette fonction peut effectuer des appels réseau vers des ressources telles que des compartiments Amazon S3, des tables DynamoDB ou des instances Amazon EC2 dans Régions AWS.	30 secondes

Quotas selon le type d'événement

Entité	Événements de demande de l'utilisateur et de réponse à l'utilisateur	Événements de demande de l'origine et de réponse à l'origine
Taille d'une réponse qui est générée par une fonction Lambda, en-têtes et corps compris	40 Ko	1 Mo

Remarques

- Pour obtenir la liste des quotas Lambda @Edge supplémentaires qui peuvent être augmentés à partir de Service Quotas, consultez la section CloudFrontPoints de terminaison et quotas Amazon dans le. Références générales AWS
- Outre ces quotas, d'autres restrictions s'appliquent lors de l'utilisation des fonctions Lambda@Edge. Pour plus d'informations, consultez Restrictions sur Lambda@Edge.

Quotas sur les certificats SSL

Entité	Quota par défaut
Certificats SSL utilisés Compte AWS lors de l'envoi de requêtes HTTPS à l'aide d'adresses IP dédiées (aucun quota lors du traitement de requêtes HTTPS via SNI) Pour plus d'informations, consultez Utilisez le protocole HTTPS avec CloudFront.	2 Demander une augmentation du quota
Certificats SSL pouvant être associés à une CloudFront distribution	1

Si votre certificat SSL est spécifiquement destiné à la communication HTTPS entre les utilisateurs et CloudFront que vous avez utilisé AWS Certificate Manager (ACM) ou le magasin de certificats IAM pour approvisionner ou importer votre certificat, des quotas supplémentaires s'appliquent. Pour plus d'informations, consultez Quotas d'utilisation de SSL/TLS certificats avec CloudFront (HTTPS entre spectateurs et CloudFront uniquement).

Il existe également des quotas sur le nombre de certificats SSL que vous pouvez importer dans AWS Certificate Manager (ACM) ou télécharger vers Gestion des identités et des accès AWS (IAM). Pour plus d'informations, consultez Augmenter les quotas de SSL/TLS certificats.

Quotas sur les invalidations

Entité	Quota par défaut
Nombre de chemins ou de balises Pour plus d'informations, consultez Invalidation de fichiers pour supprimer du contenu et Invalidation de contenu par des balises de cache.	150 chemins ou balises par seconde
Nombre d'invalidations par caractère générique	1 invalidation joker par seconde

Entité	Quota par défaut
Invalidation des balises : nombre maximum de fichiers qu'une invalidation basée sur une balise peut traiter	Pas de quota
Invalidation par caractère générique : nombre maximum de fichiers qu'une invalidation par caractère générique peut traiter	Pas de quota

Quotas sur les groupes clés

Entité	Quota par défaut
Clés publiques dans un seul groupe clé	5 Demander une augmentation du quota
Groupes clés associés à un seul comportement du cache	4 Demander une augmentation du quota
Groupes clés par Compte AWS	10 Demander une augmentation du quota
Répartitions associées à un seul groupe clé	100 Demander une augmentation du quota

Quotas sur WebSocket les connexions

Entité	Quota par défaut
Délai de réponse de l'origine (délai d'inactivité)	10 minutes Si aucun octet CloudFront n'a été détecté depuis l'origine vers le client au cours des 10 dernières minutes, la connexion est considérée comme inactive et est fermée.

Quotas sur le chiffrement au niveau du champ

Entité	Quota par défaut
Longueur maximale d'un champ à chiffrer Pour plus d’informations, consultez Utilisation du chiffrement au niveau du champ pour faciliter la protection des données sensibles.	16 Ko
Nombre maximal de champs dans le corps d'une requête lorsque le chiffrement au niveau du champ est configuré	10
Longueur maximale du corps d'une demande lorsque le chiffrement au niveau du champ est configuré	1 Mo
Nombre maximal de configurations de chiffrement au niveau du champ pouvant être associées à une Compte AWS	10
Nombre maximal de profils de chiffrement au niveau du champ pouvant être associés à un Compte AWS	10

Entité	Quota par défaut
Nombre maximal de clés publiques qui peuvent être ajoutées à un Compte AWS	10
Nombre maximum de champs à chiffrer qui peuvent être spécifiés dans un profil	10
Nombre maximal de CloudFront distributions pouvant être associées à une configuration de chiffrement au niveau du champ	20
Nombre maximum de mappages de profil d'argument de requête qui peuvent être inclus dans une configuration de chiffrement au niveau du champ	5

Quotas sur les cookies (paramètres de cache hérités)

Ces quotas s'appliquent aux CloudFront anciens paramètres de cache. Nous vous recommandons d'utiliser une politique de cache ou une politique de demande d'origine au lieu des paramètres hérités.

Entité	Quota par défaut
Cookies par comportement du cache Pour plus d'informations, consultez Mise en cache de contenu basée sur des cookies.	10 Demander une augmentation du quota
Nombre total d'octets dans les noms des cookies (ne s'applique pas si vous configurez CloudFront pour transférer tous les cookies à l'origine)	512 moins le nombre de cookies

Quotas sur les chaînes de requêtes (paramètres de cache hérités)

Ces quotas s'appliquent aux CloudFront anciens paramètres de cache. Nous vous recommandons d'utiliser une politique de cache ou une politique de demande d'origine au lieu des paramètres hérités.

Entité	Quota par défaut
Nombre maximal de caractères dans une chaîne de requêtes	128 caractères
Le nombre maximal de caractères au total pour toutes les chaînes de requêtes dans le même paramètre	512 caractères
Chaînes de requêtes par comportement du cache Pour plus d'informations, consultez Mise en cache de contenu basée sur les paramètres de chaîne de requête.	10 Demander une augmentation du quota

Quotas sur les en-têtes

Entité	Quota par défaut
En-têtes par comportement du cache (paramètres de cache hérités) Pour plus d'informations, consultez the section called "Mise en cache de contenu basée sur des en-têtes de demandes".	10 Demander une augmentation du quota
Transfert d'en-têtes par comportement de mise en cache	25 Demander une augmentation du quota
En-têtes personnalisés : nombre maximum d'en-têtes personnalisés que vous pouvez configurer CloudFront pour ajouter aux demandes d'origine Pour plus d'informations, consultez the section called "Ajout d'en-têtes personnalisés aux demandes d'origine".	30 Demander une augmentation du quota
En-têtes personnalisés : nombre maximal d'en-têtes personnalisés que vous pouvez ajouter à une politique d'en-têtes de réponses	10

Entité	Quota par défaut
	Demander une augmentation du quota
En-têtes personnalisés : longueur maximale d'un nom d'en-tête	256 caractères
En-têtes personnalisés : longueur maximale d'une valeur d'en-tête	1,783 caractères
En-têtes personnalisés : longueur maximale de tous les noms et valeurs d'en-tête combinés	10 240 caractères
Longueur maximale de la valeur de l'en-tête `Content-Security-Policy`	1 783 caractères Demander une augmentation du quota
Longueur maximale d'une valeur d'en-tête `CORS (Access-Control-Allow-Origin)`	1 783 caractères

Quotas sur les distributions multi-locataires

Entité	Quota par défaut
Nombre maximum de locataires de distribution par Compte AWS	10 000 Demander une augmentation du quota
Nombre maximum de distributions multi-locataires par Compte AWS	20 Demander une augmentation du quota
Nombre maximum de groupes de connexions par Compte AWS	100

Entité	Quota par défaut
	Demander une augmentation du quota
Nombre maximal d'alias par locataire de distribution	100 Demander une augmentation du quota
Nombre maximal de paramètres par locataire de distribution	5 Demander une augmentation du quota
Nombre maximal de paramètres par distribution multi-locataires	5 Demander une augmentation du quota
Nombre maximal de paramètres dans un champ d'une distribution multi-locataires	2 Demander une augmentation du quota
Nombre maximum de groupes de connexions par liste d'adresses IP statiques en unidiffusion	5 Demander une augmentation du quota

Pour plus d'informations sur les distributions multi-locataires, consultez Compréhension du fonctionnement des distributions multi-locataires.

Informations connexes

Pour plus d'informations, consultez la section CloudFront Points de terminaison et quotas Amazon dans le Références générales AWS.

Exemples de code à CloudFront utiliser AWS Kits SDK

Les exemples de code suivants montrent comment utiliser CloudFront un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés.

Les scénarios sont des exemples de code qui vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'un même service ou combinés à d'autres Services AWS.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Exemples de base pour CloudFront l'utilisation AWS Kits SDK
  - Actions d' CloudFront utilisation AWS Kits SDK
    - À utiliser CreateDistributionavec un AWS SDK ou CLI
    - À utiliser CreateFunctionavec un AWS Kit SDK
    - Utilisation de CreateInvalidation avec une CLI
    - À utiliser CreateKeyGroupavec un AWS Kit SDK
    - À utiliser CreatePublicKeyavec un AWS SDK ou CLI
    - À utiliser DeleteDistributionavec un AWS SDK ou CLI
    - Utilisation de GetCloudFrontOriginAccessIdentity avec une CLI
    - Utilisation de GetCloudFrontOriginAccessIdentityConfig avec une CLI
    - Utilisation de GetDistribution avec une CLI
    - À utiliser GetDistributionConfigavec un AWS SDK ou CLI
    - Utilisation de ListCloudFrontOriginAccessIdentities avec une CLI
    - À utiliser ListDistributionsavec un AWS SDK ou CLI
    - À utiliser UpdateDistributionavec un AWS SDK ou CLI

- Scénarios d' CloudFront utilisation AWS Kits SDK
  - Créez des ressources pour les gestionnaires SaaS AWS Kit SDK
  - Supprimer les ressources CloudFront de signature à l'aide de AWS Kit SDK
  - Commencez avec un réseau de distribution de contenu de base
  - Commencer à utiliser les pare-feux pour applications Web
  - Créez des URL signées et des cookies à l'aide d'un AWS Kit SDK
- CloudFront Exemples de fonctions pour CloudFront
  - Ajouter des en-têtes de sécurité HTTP à un événement de réponse du visualiseur CloudFront Functions
  - Ajouter un en-tête CORS à un événement de réponse de l'afficheur de CloudFront fonctions
  - Ajouter un en-tête de contrôle du cache à un événement de réponse du visualiseur CloudFront Functions
  - Ajouter un véritable en-tête IP client à un événement de demande du visualiseur CloudFront Functions
  - Ajouter un en-tête d'origine à un événement de demande d'affichage de CloudFront fonctions
  - Ajoutez index.html pour demander des URL sans nom de fichier dans un événement de demande de l'afficheur CloudFront Functions
  - Normaliser les paramètres de chaîne de requête dans une demande d'affichage de CloudFront fonctions
  - Redirection vers une nouvelle URL dans un événement de demande de l'afficheur CloudFront Functions
  - Réécriture d'une URI de demande en fonction de la KeyValueStore configuration d'un événement de demande du visualiseur de CloudFront fonctions
  - Acheminer les demandes vers une origine plus proche du visualiseur dans un événement de demande du visualiseur CloudFront Functions
  - Utiliser des paires clé-valeur dans une demande d'affichage de CloudFront fonctions
  - Valider un jeton simple dans une demande d'affichage de CloudFront fonctions

Exemples de base pour CloudFront l'utilisation AWS Kits SDK

Les exemples de code suivants montrent comment utiliser les bases d'Amazon CloudFront avec AWS les SDK.

Exemples

- Actions d' CloudFront utilisation AWS Kits SDK
  - À utiliser CreateDistributionavec un AWS SDK ou CLI
  - À utiliser CreateFunctionavec un AWS Kit SDK
  - Utilisation de CreateInvalidation avec une CLI
  - À utiliser CreateKeyGroupavec un AWS Kit SDK
  - À utiliser CreatePublicKeyavec un AWS SDK ou CLI
  - À utiliser DeleteDistributionavec un AWS SDK ou CLI
  - Utilisation de GetCloudFrontOriginAccessIdentity avec une CLI
  - Utilisation de GetCloudFrontOriginAccessIdentityConfig avec une CLI
  - Utilisation de GetDistribution avec une CLI
  - À utiliser GetDistributionConfigavec un AWS SDK ou CLI
  - Utilisation de ListCloudFrontOriginAccessIdentities avec une CLI
  - À utiliser ListDistributionsavec un AWS SDK ou CLI
  - À utiliser UpdateDistributionavec un AWS SDK ou CLI

Actions d' CloudFront utilisation AWS Kits SDK

Les exemples de code suivants montrent comment effectuer des CloudFront actions individuelles avec AWS les SDK. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Ces extraits appellent l' CloudFront API et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Vous pouvez voir les actions dans leur contexte dans Scénarios d' CloudFront utilisation AWS Kits SDK.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une liste complète, consultez le Amazon CloudFront API Reference.

Exemples

- À utiliser CreateDistributionavec un AWS SDK ou CLI
- À utiliser CreateFunctionavec un AWS Kit SDK
- Utilisation de CreateInvalidation avec une CLI
- À utiliser CreateKeyGroupavec un AWS Kit SDK

- À utiliser CreatePublicKeyavec un AWS SDK ou CLI
- À utiliser DeleteDistributionavec un AWS SDK ou CLI
- Utilisation de GetCloudFrontOriginAccessIdentity avec une CLI
- Utilisation de GetCloudFrontOriginAccessIdentityConfig avec une CLI
- Utilisation de GetDistribution avec une CLI
- À utiliser GetDistributionConfigavec un AWS SDK ou CLI
- Utilisation de ListCloudFrontOriginAccessIdentities avec une CLI
- À utiliser ListDistributionsavec un AWS SDK ou CLI
- À utiliser UpdateDistributionavec un AWS SDK ou CLI

À utiliser **`CreateDistribution`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `CreateDistribution`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Création d'une distribution à locataires multiples et d'un locataire de distribution
- Commencez avec un réseau de distribution de contenu de base

CLI

AWS CLI

Exemple 1 : pour créer une CloudFront distribution

L'exemple `create-distribution` suivant crée une distribution pour un compartiment S3 nommé `amzn-s3-demo-bucket`, et spécifie également `index.html` comme objet racine par défaut, à l'aide d'arguments de ligne de commande.

```
aws cloudfront create-distribution \
    --origin-domain-name amzn-s3-demo-bucket.s3.amazonaws.com \
    --default-root-object index.html
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EMLARXS9EXAMPLE",
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-11-22T00:55:15.705Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-
example",
```

```
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
```

```
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

Exemple 2 : pour créer une CloudFront distribution à l'aide d'un fichier JSON

L'exemple `create-distribution` suivant crée une distribution pour un compartiment S3 nommé `amzn-s3-demo-bucket`, et spécifie également `index.html` comme objet racine par défaut, à l'aide d'un fichier JSON.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenu de `dist-config.json` :

```
{
    "CallerReference": "cli-example",
```

```
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
```

```
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": true,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
```

```
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
}
```

Consultez l'exemple 1 pour un exemple de sortie.

Exemple 3 : pour créer une distribution CloudFront multi-locataires avec un certificat

L'`create-distribution`exemple suivant crée une CloudFront distribution prenant en charge plusieurs locataires et spécifie un certificat TLS.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenu de `dist-config.json` :

```
{
    "CallerReference": "cli-example-with-cert",
    "Comment": "CLI example distribution",
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
```

```
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["HEAD", "GET"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["HEAD", "GET"]
            }
        }
    },
    "Enabled": true,
    "ViewerCertificate": {
        "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/191306a1-db01-49ca-90ef-fc414ee5dabc",
        "SSLSupportMethod": "sni-only"
    },
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
        ]
    }
}
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E1HVIAU7UABC",
    "ETag": "E20LT7R1BABC",
    "Distribution": {
        "Id": "E1HVIAU7U12ABC",
```

```
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E1HVIAU7U12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:33:31.117000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example-with-cert",
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": ""
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
```

```
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": ["HEAD", "GET"],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": ["HEAD", "GET"]
                    }
                },
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
                "GrpcConfig": {
                    "Enabled": false
                }
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "CLI example distribution",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": false,
```

```
                "ACMCertificateArn": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "SSLSupportMethod": "sni-only",
                "MinimumProtocolVersion": "TLSv1.2_2021",
                "Certificate": "arn:aws:acm:us-
east-1:123456789012:certificate/1954f095-11b6-4daf-9952-0c308a00abc",
                "CertificateSource": "acm"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
        }
    }
}
```

Pour plus d'informations, consultez la section Travailler avec les distributions dans le manuel Amazon CloudFront Developer Guide.

Exemple 4 : pour créer une distribution CloudFront multi-locataires sans certificat

L'`create-distribution`exemple suivant crée une CloudFront distribution prenant en charge plusieurs locataires mais sans certificat TLS.

```
aws cloudfront create-distribution \
    --distribution-config file://dist-config.json
```

Contenu de `dist-config.json` :

```
{
    "CallerReference": "cli-example",
    "Comment": "CLI example distribution",
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "DomainName": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                "OriginPath": "/{{tenantName}}",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
        "ViewerProtocolPolicy": "allow-all",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        }
```

```
    },
    "Enabled": true,
    "HttpVersion": "http2",
    "ConnectionMode": "tenant-only",
    "TenantConfig": {
        "ParameterDefinitions": [
            {
                "Name": "tenantName",
                "Definition": {
                    "StringSchema": {
                        "Comment": "tenantName parameter",
                        "DefaultValue": "root",
                        "Required": false
                    }
                }
            }
        ]
    }
}
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2020-05-31/distribution/
E2GJ5J9QN12ABC",
    "ETag": "E37YLVVQIABC",
    "Distribution": {
        "Id": "E2GJ5J9QNABC",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/E2GJ5J9QN12ABC",
        "Status": "InProgress",
        "LastModifiedTime": "2025-07-10T20:35:20.565000+00:00",
        "InProgressInvalidationBatches": 0,
        "DomainName": "example.com",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ActiveTrustedKeyGroups": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-example-no-cert",
```

```
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.us-east-1.amazonaws.com",
                        "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                        "OriginPath": "/{{tenantName}}",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        },
                        "ConnectionAttempts": 3,
                        "ConnectionTimeout": 10,
                        "OriginShield": {
                            "Enabled": false
                        },
                        "OriginAccessControlId": ""
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                "TrustedKeyGroups": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
```

```
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": "",
            "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e5ABC",
            "GrpcConfig": {
                "Enabled": false
            }
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "CLI example distribution",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
            "SSLSupportMethod": "sni-only",
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
        },
```

```
            "WebACLId": "",
            "HttpVersion": "http2",
            "TenantConfig": {
                "ParameterDefinitions": [
                    {
                        "Name": "tenantName",
                        "Definition": {
                            "StringSchema": {
                                "Comment": "tenantName parameter",
                                "DefaultValue": "root",
                                "Required": false
                            }
                        }
                    }
                ]
            },
            "ConnectionMode": "tenant-only"
        }
    }
}
```

Pour plus d'informations, consultez Configurer les distributions dans le manuel Amazon CloudFront Developer Guide.

- Pour plus de détails sur l'API, reportez-vous CreateDistributionà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

L'exemple suivant utilise un compartiment Amazon Simple Storage Service (Amazon S3) comme origine de contenu.

Après avoir créé la distribution, le code crée un CloudFrontWaiterpour attendre que la distribution soit déployée avant de renvoyer la distribution.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.core.internal.waiters.ResponseOrException;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.Distribution;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.ItemSelection;
import software.amazon.awssdk.services.cloudfront.model.Method;
import software.amazon.awssdk.services.cloudfront.model.ViewerProtocolPolicy;
import software.amazon.awssdk.services.cloudfront.waiters.CloudFrontWaiter;
import software.amazon.awssdk.services.s3.S3Client;

import java.time.Instant;

public class CreateDistribution {

        private static final Logger logger =
 LoggerFactory.getLogger(CreateDistribution.class);

        public static Distribution createDistribution(CloudFrontClient
 cloudFrontClient, S3Client s3Client,
                        final String bucketName, final String keyGroupId, final
 String originAccessControlId) {

                final String region = s3Client.headBucket(b ->
 b.bucket(bucketName)).sdkHttpResponse().headers()
                                .get("x-amz-bucket-region").get(0);
                final String originDomain = bucketName + ".s3." + region +
 ".amazonaws.com";
                String originId = originDomain; // Use the originDomain value for
 the originId.

                // The service API requires some deprecated methods, such as
                // DefaultCacheBehavior.Builder#minTTL and #forwardedValue.
                CreateDistributionResponse createDistResponse =
 cloudFrontClient.createDistribution(builder -> builder
                                .distributionConfig(b1 -> b1
                                                .origins(b2 -> b2
                                                                .quantity(1)
                                                                .items(b3 -> b3
```

```
.domainName(originDomain)

.id(originId)

.s3OriginConfig(builder4 -> builder4

              .originAccessIdentity(

                                 ""))

.originAccessControlId(

              originAccessControlId)))
                                                  .defaultCacheBehavior(b2 -> b2

.viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)

.targetOriginId(originId)
                                                                        .minTTL(200L)

.forwardedValues(b5 -> b5

.cookies(cp -> cp

              .forward(ItemSelection.NONE))

.queryString(true))

.trustedKeyGroups(b3 -> b3

.quantity(1)

.items(keyGroupId)

.enabled(true))

.allowedMethods(b4 -> b4

.quantity(2)

.items(Method.HEAD, Method.GET)

.cachedMethods(b5 -> b5
```

```
                .quantity(2)
                .items(Method.HEAD,
                                Method.GET))))
                                                .cacheBehaviors(b -> b
                                                                .quantity(1)
                                                                .items(b2 -> b2
.pathPattern("/index.html")
.viewerProtocolPolicy(
                ViewerProtocolPolicy.ALLOW_ALL)
.targetOriginId(originId)
.trustedKeyGroups(b3 -> b3
                .quantity(1)
                .items(keyGroupId)
                .enabled(true))
.minTTL(200L)
.forwardedValues(b4 -> b4
                .cookies(cp -> cp
                                .forward(ItemSelection.NONE))
                .queryString(true))
.allowedMethods(b5 -> b5.quantity(2)
                .items(Method.HEAD,
                                Method.GET)
                .cachedMethods(b6 -> b6
```

```
                                .quantity(2)

                                .items(Method.HEAD,

                                                Method.GET)))))
                                 .enabled(true)
                                 .comment("Distribution built with
 java")

 .callerReference(Instant.now().toString())));

                final Distribution distribution =
 createDistResponse.distribution();
                logger.info("Distribution created. DomainName: [{}]  Id: [{}]",
 distribution.domainName(),
                                 distribution.id());
                logger.info("Waiting for distribution to be deployed ...");
                try (CloudFrontWaiter cfWaiter =
 CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
                        ResponseOrException<GetDistributionResponse>
 responseOrException = cfWaiter
                                        .waitUntilDistributionDeployed(builder ->
 builder.id(distribution.id()))
                                        .matched();
                        responseOrException.response()
                                        .orElseThrow(() -> new
 RuntimeException("Distribution not created"));
                        logger.info("Distribution deployed. DomainName: [{}]  Id:
 [{}]", distribution.domainName(),
                                        distribution.id());
                }
                return distribution;
        }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateDistributionà la section Référence des AWS SDK for Java 2.x API.

PowerShell

Outils pour PowerShell V4

Exemple 1 : crée une CloudFront distribution de base, configurée avec la journalisation et la mise en cache.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "amzn-s3-demo-bucket.s3.amazonaws.com"
$origin.Id = "UniqueOrigin1"
$origin.S3OriginConfig = New-Object Amazon.CloudFront.Model.S3OriginConfig
$origin.S3OriginConfig.OriginAccessIdentity = ""
New-CFDistribution `
      -DistributionConfig_Enabled $true `
      -DistributionConfig_Comment "Test distribution" `
      -Origins_Item $origin `
      -Origins_Quantity 1 `
      -Logging_Enabled $true `
      -Logging_IncludeCookie $true `
      -Logging_Bucket amzn-s3-demo-logging-bucket.s3.amazonaws.com `
      -Logging_Prefix "help/" `
      -DistributionConfig_CallerReference Client1 `
      -DistributionConfig_DefaultRootObject index.html `
      -DefaultCacheBehavior_TargetOriginId $origin.Id `
      -ForwardedValues_QueryString $true `
      -Cookies_Forward all `
      -WhitelistedNames_Quantity 0 `
      -TrustedSigners_Enabled $false `
      -TrustedSigners_Quantity 0 `
      -DefaultCacheBehavior_ViewerProtocolPolicy allow-all `
      -DefaultCacheBehavior_MinTTL 1000 `
      -DistributionConfig_PriceClass "PriceClass_All" `
      -CacheBehaviors_Quantity 0 `
      -Aliases_Quantity 0
```

- Pour plus de détails sur l'API, reportez-vous CreateDistributionà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : crée une CloudFront distribution de base, configurée avec la journalisation et la mise en cache.

```
$origin = New-Object Amazon.CloudFront.Model.Origin
$origin.DomainName = "amzn-s3-demo-bucket.s3.amazonaws.com"
$origin.Id = "UniqueOrigin1"
$origin.S3OriginConfig = New-Object Amazon.CloudFront.Model.S3OriginConfig
$origin.S3OriginConfig.OriginAccessIdentity = ""
New-CFDistribution `
      -DistributionConfig_Enabled $true `
      -DistributionConfig_Comment "Test distribution" `
      -Origins_Item $origin `
      -Origins_Quantity 1 `
      -Logging_Enabled $true `
      -Logging_IncludeCookie $true `
      -Logging_Bucket amzn-s3-demo-logging-bucket.s3.amazonaws.com `
      -Logging_Prefix "help/" `
      -DistributionConfig_CallerReference Client1 `
      -DistributionConfig_DefaultRootObject index.html `
      -DefaultCacheBehavior_TargetOriginId $origin.Id `
      -ForwardedValues_QueryString $true `
      -Cookies_Forward all `
      -WhitelistedNames_Quantity 0 `
      -TrustedSigners_Enabled $false `
      -TrustedSigners_Quantity 0 `
      -DefaultCacheBehavior_ViewerProtocolPolicy allow-all `
      -DefaultCacheBehavior_MinTTL 1000 `
      -DistributionConfig_PriceClass "PriceClass_All" `
      -CacheBehaviors_Quantity 0 `
      -Aliases_Quantity 0
```

- Pour plus de détails sur l'API, reportez-vous CreateDistributionà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`CreateFunction`**avec un AWS Kit SDK

L'exemple de code suivant montre comment utiliser`CreateFunction`.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.CloudFrontException;
import software.amazon.awssdk.services.cloudfront.model.CreateFunctionRequest;
import software.amazon.awssdk.services.cloudfront.model.CreateFunctionResponse;
import software.amazon.awssdk.services.cloudfront.model.FunctionConfig;
import software.amazon.awssdk.services.cloudfront.model.FunctionRuntime;
import java.io.InputStream;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateFunction {

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <functionName> <filePath>

                Where:
                    functionName - The name of the function to create.\s
                    filePath - The path to a file that contains the application
 logic for the function.\s
                """;
```

```
        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        String filePath = args[1];
        CloudFrontClient cloudFrontClient = CloudFrontClient.builder()
                .region(Region.AWS_GLOBAL)
                .build();

        String funArn = createNewFunction(cloudFrontClient, functionName,
filePath);
        System.out.println("The function ARN is " + funArn);
        cloudFrontClient.close();
    }

    public static String createNewFunction(CloudFrontClient cloudFrontClient,
String functionName, String filePath) {
        try {
            InputStream fileIs =
CreateFunction.class.getClassLoader().getResourceAsStream(filePath);
            SdkBytes functionCode = SdkBytes.fromInputStream(fileIs);

            FunctionConfig config = FunctionConfig.builder()
                    .comment("Created by using the CloudFront Java API")
                    .runtime(FunctionRuntime.CLOUDFRONT_JS_1_0)
                    .build();

            CreateFunctionRequest functionRequest =
CreateFunctionRequest.builder()
                    .name(functionName)
                    .functionCode(functionCode)
                    .functionConfig(config)
                    .build();

            CreateFunctionResponse response =
cloudFrontClient.createFunction(functionRequest);
            return response.functionSummary().functionMetadata().functionARN();

        } catch (CloudFrontException e) {
            System.err.println(e.getMessage());
            System.exit(1);
```

```
        }
        return "";
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateFunctionà la section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`CreateInvalidation`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `CreateInvalidation`.

CLI

AWS CLI

Pour créer une invalidation pour une distribution CloudFront

L'`create-invalidation`exemple suivant crée une invalidation pour les fichiers spécifiés dans la CloudFront distribution spécifiée :

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --paths "/example-path/example-file.jpg" "/example-path/example-file2.png"
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EDFDVBD6EXAMPLE/invalidation/I1JLWSDAP8FU89",
    "Invalidation": {
        "Id": "I1JLWSDAP8FU89",
        "Status": "InProgress",
        "CreateTime": "2019-12-05T18:24:51.407Z",
        "InvalidationBatch": {
            "Paths": {
```

```
                "Quantity": 2,
                "Items": [
                    "/example-path/example-file2.png",
                    "/example-path/example-file.jpg"
                ]
            },
            "CallerReference": "cli-1575570291-670203"
        }
    }
}
```

Dans l'exemple précédent, la AWS CLI a automatiquement généré un résultat aléatoire`CallerReference`. Pour spécifier votre propre `CallerReference` ou pour éviter de transmettre les paramètres d'invalidation en tant qu'arguments de ligne de commande, vous pouvez utiliser un fichier JSON. L'exemple suivant crée une invalidation pour deux fichiers, en fournissant les paramètres d'invalidation dans un fichier JSON nommé `inv-batch.json` :

```
aws cloudfront create-invalidation \
    --distribution-id EDFDVBD6EXAMPLE \
    --invalidation-batch file://inv-batch.json
```

Contenu de `inv-batch.json` :

```
{
    "Paths": {
        "Quantity": 2,
        "Items": [
            "/example-path/example-file.jpg",
            "/example-path/example-file2.png"
        ]
    },
    "CallerReference": "cli-example"
}
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/distribution/
EDFDVBD6EXAMPLE/invalidation/I2J0I21PCUYOIK",
    "Invalidation": {
```

```
        "Id": "I2J0I21PCUYOIK",
        "Status": "InProgress",
        "CreateTime": "2019-12-05T18:40:49.413Z",
        "InvalidationBatch": {
            "Paths": {
                "Quantity": 2,
                "Items": [
                    "/example-path/example-file.jpg",
                    "/example-path/example-file2.png"
                ]
            },
            "CallerReference": "cli-example"
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateInvalidationà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cet exemple crée une invalidation sur une distribution dont l'ID est EXAMPLENSTXAXE. CallerReference Il s'agit d'un identifiant unique choisi par l'utilisateur ; dans ce cas, un horodatage représentant le 15 mai 2019 à 9 h 00 est utilisé. La variable $Paths stocke trois chemins vers des fichiers image et média que l'utilisateur ne souhaite pas inclure dans le cache de la distribution. La valeur du Paths_Quantity paramètre - est le nombre total de chemins spécifiés dans le Paths_Item paramètre -.

```
$Paths = "/images/*.gif", "/images/image1.jpg", "/videos/*.mp4"
New-CFInvalidation -DistributionId "EXAMPLENSTXAXE" -
InvalidationBatch_CallerReference 20190515090000 -Paths_Item $Paths -
Paths_Quantity 3
```

Sortie :

```
Invalidation                        Location

------------                        --------
```

```
Amazon.CloudFront.Model.Invalidation https://cloudfront.amazonaws.com/2018-11-05/
distribution/EXAMPLENSTXAXE/invalidation/EXAMPLE8NOK9H
```

- Pour plus de détails sur l'API, reportez-vous CreateInvalidationà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cet exemple crée une invalidation sur une distribution dont l'ID est EXAMPLENSTXAXE. CallerReference Il s'agit d'un identifiant unique choisi par l'utilisateur ; dans ce cas, un horodatage représentant le 15 mai 2019 à 9 h 00 est utilisé. La variable $Paths stocke trois chemins vers des fichiers image et média que l'utilisateur ne souhaite pas inclure dans le cache de la distribution. La valeur du Paths_Quantity paramètre - est le nombre total de chemins spécifiés dans le Paths_Item paramètre -.

```
$Paths = "/images/*.gif", "/images/image1.jpg", "/videos/*.mp4"
New-CFInvalidation -DistributionId "EXAMPLENSTXAXE" -
InvalidationBatch_CallerReference 20190515090000 -Paths_Item $Paths -
Paths_Quantity 3
```

Sortie :

```
Invalidation                        Location

------------                        --------

Amazon.CloudFront.Model.Invalidation https://cloudfront.amazonaws.com/2018-11-05/
distribution/EXAMPLENSTXAXE/invalidation/EXAMPLE8NOK9H
```

- Pour plus de détails sur l'API, reportez-vous CreateInvalidationà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`CreateKeyGroup`**avec un AWS Kit SDK

L'exemple de code suivant montre comment utiliser`CreateKeyGroup`.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Un groupe de clés nécessite au moins une clé publique utilisée pour vérifier les URL signées ou les cookies.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;

import java.util.UUID;

public class CreateKeyGroup {
    private static final Logger logger =
 LoggerFactory.getLogger(CreateKeyGroup.class);

    public static String createKeyGroup(CloudFrontClient cloudFrontClient, String
 publicKeyId) {
        String keyGroupId = cloudFrontClient.createKeyGroup(b ->
 b.keyGroupConfig(c -> c
                .items(publicKeyId)
                .name("JavaKeyGroup" + UUID.randomUUID())))
                .keyGroup().id();
        logger.info("KeyGroup created with ID: [{}]", keyGroupId);
        return keyGroupId;
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateKeyGroupà la section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`CreatePublicKey`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `CreatePublicKey`.

CLI

AWS CLI

Pour créer une clé CloudFront publique

L'exemple suivant crée une clé CloudFront publique en fournissant les paramètres dans un fichier JSON nommépub-key-config.json. Avant de pouvoir utiliser cette commande, vous devez disposer d'une clé PEM-encoded publique. Pour plus d'informations, consultez la section Créer une paire de clés RSA dans le manuel Amazon CloudFront Developer Guide.

```
aws cloudfront create-public-key \
    --public-key-config file://pub-key-config.json
```

Le fichier pub-key-config.json est un document JSON dans le dossier actuel qui contient ce qui suit. Notez que la clé publique est encodée au format PEM.

```
{
    "CallerReference": "cli-example",
    "Name": "ExampleKey",
    "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----
END PUBLIC KEY-----\n",
    "Comment": "example public key"
}
```

Sortie :

```
{
    "Location": "https://cloudfront.amazonaws.com/2019-03-26/public-key/
KDFB19YGCR002",
    "ETag": "E2QWRUHEXAMPLE",
    "PublicKey": {
        "Id": "KDFB19YGCR002",
        "CreatedTime": "2019-12-05T18:51:43.781Z",
        "PublicKeyConfig": {
            "CallerReference": "cli-example",
            "Name": "ExampleKey",
            "EncodedKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxPMbCA2Ks0lnd7IR+3pw
\nwd3H/7jPGwj8bLUmore7bX+oeGpZ6QmLAe/1UOWcmZX2u70dYcSIzB1ofZtcn4cJ
\nenHBAzO3ohBY/L1tQGJfS2A+omnN6H16VZE1JCK8XSJyfze7MDLcUyHZETdxuvRb
\nA9X343/vMAuQPnhinFJ8Wdy8YBXSPpy7r95ylUQd9LfYTBzVZYG2tSesplcOkjM3\n2Uu
+oMWxQAw1NINnSLPinMVsutJy6ZqlV3McWNWe4T+STGtWhrPNqJEn45sIcCx4\nq
+kGZ2NQ0FyIyT2eiLKOX5Rgb/a36E/aMk4VoDsaenBQgG7WLTnstb9sr7MIhS6A\nrwIDAQAB\n-----
END PUBLIC KEY-----\n",
            "Comment": "example public key"
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreatePublicKeyà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

L'exemple de code suivant lit une clé publique et la télécharge sur Amazon CloudFront.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
```

```
import software.amazon.awssdk.services.cloudfront.model.CreatePublicKeyResponse;
import software.amazon.awssdk.utils.IoUtils;

import java.io.IOException;
import java.io.InputStream;
import java.util.UUID;

public class CreatePublicKey {
    private static final Logger logger =
 LoggerFactory.getLogger(CreatePublicKey.class);

    public static String createPublicKey(CloudFrontClient cloudFrontClient,
 String publicKeyFileName) {
        try (InputStream is =
 CreatePublicKey.class.getClassLoader().getResourceAsStream(publicKeyFileName)) {
            String publicKeyString = IoUtils.toUtf8String(is);
            CreatePublicKeyResponse createPublicKeyResponse = cloudFrontClient
                    .createPublicKey(b -> b.publicKeyConfig(c -> c
                            .name("JavaCreatedPublicKey" + UUID.randomUUID())
                            .encodedKey(publicKeyString)
                            .callerReference(UUID.randomUUID().toString())));
            String createdPublicKeyId = createPublicKeyResponse.publicKey().id();
            logger.info("Public key created with id: [{}]", createdPublicKeyId);
            return createdPublicKeyId;

        } catch (IOException e) {
            throw new RuntimeException(e);
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreatePublicKeyà la section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`DeleteDistribution`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `DeleteDistribution`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Commencez avec un réseau de distribution de contenu de base

CLI

AWS CLI

Pour supprimer une CloudFront distribution

L'exemple suivant supprime la CloudFront distribution avec l'ID. `EDFDVBD6EXAMPLE` Avant de pouvoir supprimer une distribution, vous devez la désactiver. Pour désactiver une distribution, utilisez la commande update-distribution. Pour plus d'informations, consultez les examples avec update-distribution.

Lorsqu'une distribution est désactivée, vous pouvez la supprimer. Pour supprimer une distribution, vous devez utiliser l'option `--if-match` permettant de fournir l'`ETag` de la distribution. Pour l'obtenir l'`ETag`, utilisez la commande get-distribution ou get-distribution-config.

```
aws cloudfront delete-distribution \
    --id EDFDVBD6EXAMPLE \
    --if-match E2QWRUHEXAMPLE
```

Cette commande ne produit aucune sortie lorsqu'elle réussit.

- Pour plus de détails sur l'API, reportez-vous DeleteDistributionà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

L'exemple de code suivant met à jour une distribution sur Disabled, utilise un serveur qui attend que la modification soit déployée, puis supprime la distribution.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.core.internal.waiters.ResponseOrException;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.DeleteDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionConfig;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.waiters.CloudFrontWaiter;

public class DeleteDistribution {
        private static final Logger logger =
 LoggerFactory.getLogger(DeleteDistribution.class);

        public static void deleteDistribution(final CloudFrontClient
 cloudFrontClient, final String distributionId) {
                // First, disable the distribution by updating it.
                GetDistributionResponse response =
 cloudFrontClient.getDistribution(b -> b
                                .id(distributionId));
                String etag = response.eTag();
                DistributionConfig distConfig =
 response.distribution().distributionConfig();

                cloudFrontClient.updateDistribution(builder -> builder
                                .id(distributionId)
                                .distributionConfig(builder1 -> builder1

 .cacheBehaviors(distConfig.cacheBehaviors())

 .defaultCacheBehavior(distConfig.defaultCacheBehavior())
                                                        .enabled(false)
                                                        .origins(distConfig.origins())
                                                        .comment(distConfig.comment())

 .callerReference(distConfig.callerReference())

 .defaultCacheBehavior(distConfig.defaultCacheBehavior())

 .priceClass(distConfig.priceClass())
```

```
                                                .aliases(distConfig.aliases())
                                                .logging(distConfig.logging())

.defaultRootObject(distConfig.defaultRootObject())

.customErrorResponses(distConfig.customErrorResponses())

.httpVersion(distConfig.httpVersion())

.isIPV6Enabled(distConfig.isIPV6Enabled())

.restrictions(distConfig.restrictions())

.viewerCertificate(distConfig.viewerCertificate())
                                                .webACLId(distConfig.webACLId())

.originGroups(distConfig.originGroups()))
                                .ifMatch(etag));

                logger.info("Distribution [{}] is DISABLED, waiting for
deployment before deleting ...",
                                distributionId);
                GetDistributionResponse distributionResponse;
                try (CloudFrontWaiter cfWaiter =
CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
                        ResponseOrException<GetDistributionResponse>
responseOrException = cfWaiter
                                        .waitUntilDistributionDeployed(builder ->
builder.id(distributionId)).matched();
                        distributionResponse = responseOrException.response()
                                        .orElseThrow(() -> new
RuntimeException("Could not disable distribution"));
                }

                DeleteDistributionResponse deleteDistributionResponse =
cloudFrontClient
                                .deleteDistribution(builder -> builder
                                                .id(distributionId)

.ifMatch(distributionResponse.eTag()));
                if (deleteDistributionResponse.sdkHttpResponse().isSuccessful())
{
                        logger.info("Distribution [{}] DELETED", distributionId);
                }
```

```
        }
}
```

- Pour plus de détails sur l'API, reportez-vous DeleteDistributionà la section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetCloudFrontOriginAccessIdentity`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetCloudFrontOriginAccessIdentity`.

CLI

AWS CLI

Pour obtenir une identité CloudFront d'accès à l'origine

L'exemple suivant obtient l'identité CloudFront d'accès à l'origine (OAI) avec l'IDE74FTE3AEXAMPLE, y compris son identifiant canonique S3 ETag et l'identifiant canonique S3 associé. L'ID de l'OAI est renvoyé dans la sortie des commandes create-cloud-front-origin-access-identity et list-cloud-front-origin-access-identity.

```
aws cloudfront get-cloud-front-origin-access-identity --id E74FTE3AEXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentity": {
        "Id": "E74FTE3AEXAMPLE",
        "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
        "CloudFrontOriginAccessIdentityConfig": {
            "CallerReference": "cli-example",
            "Comment": "Example OAI"
        }
```

```
    }
}
```

- Pour plus de détails sur l'API, reportez-vous GetCloudFrontOriginAccessIdentityà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cet exemple renvoie une identité d'accès Amazon CloudFront Origin spécifique, spécifiée par le paramètre -Id. Bien que le paramètre -Id ne soit pas obligatoire, aucun résultat n'est renvoyé si vous ne le spécifiez pas.

```
Get-CFCloudFrontOriginAccessIdentity -Id E3XXXXXXXXXXRT
```

Sortie :

```
 CloudFrontOriginAccessIdentityConfig    Id
S3CanonicalUserId
 ------------------------------------    --
-----------------
 Amazon.CloudFront.Model.CloudFrontOr... E3XXXXXXXXXXRT
4b6e...
```

- Pour plus de détails sur l'API, reportez-vous GetCloudFrontOriginAccessIdentityà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cet exemple renvoie une identité d'accès Amazon CloudFront Origin spécifique, spécifiée par le paramètre -Id. Bien que le paramètre -Id ne soit pas obligatoire, aucun résultat n'est renvoyé si vous ne le spécifiez pas.

```
Get-CFCloudFrontOriginAccessIdentity -Id E3XXXXXXXXXXRT
```

Sortie :

```
 CloudFrontOriginAccessIdentityConfig    Id
S3CanonicalUserId
```

```
     ------------------------------------    --
    -----------------
     Amazon.CloudFront.Model.CloudFrontOr... E3XXXXXXXXXXRT
    4b6e...
```

- Pour plus de détails sur l'API, reportez-vous GetCloudFrontOriginAccessIdentityà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetCloudFrontOriginAccessIdentityConfig`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetCloudFrontOriginAccessIdentityConfig`.

CLI

AWS CLI

Pour obtenir une configuration d'identité CloudFront d'accès à l'origine

L'exemple suivant obtient des métadonnées relatives à l'identité CloudFront d'accès à l'origine (OAI) avec l'IDE74FTE3AEXAMPLE, y compris sonETag. L'ID de l'OAI est renvoyé dans la sortie des commandes create-cloud-front-origin-access-identity et list-cloud-front-origin-access-identity.

```
aws cloudfront get-cloud-front-origin-access-identity-config --id E74FTE3AEXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "CloudFrontOriginAccessIdentityConfig": {
        "CallerReference": "cli-example",
        "Comment": "Example OAI"
    }
}
```

- Pour plus de détails sur l'API, reportez-vous GetCloudFrontOriginAccessIdentityConfigà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cet exemple renvoie des informations de configuration concernant une seule identité CloudFront d'accès à Amazon Origin, spécifiée par le paramètre -Id. Des erreurs se produisent si aucun paramètre -Id n'est spécifié.

```
Get-CFCloudFrontOriginAccessIdentityConfig -Id E3XXXXXXXXXXRT
```

Sortie :

```
     CallerReference                                                Comment
     ---------------                                                -------
     mycallerreference: 2/1/2011 1:16:32 PM                         Caller
reference: 2/1/2011 1:16:32 PM
```

- Pour plus de détails sur l'API, reportez-vous GetCloudFrontOriginAccessIdentityConfigà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cet exemple renvoie des informations de configuration concernant une seule identité CloudFront d'accès à Amazon Origin, spécifiée par le paramètre -Id. Des erreurs se produisent si aucun paramètre -Id n'est spécifié.

```
Get-CFCloudFrontOriginAccessIdentityConfig -Id E3XXXXXXXXXXRT
```

Sortie :

```
     CallerReference                                                Comment
     ---------------                                                -------
     mycallerreference: 2/1/2011 1:16:32 PM                         Caller
reference: 2/1/2011 1:16:32 PM
```

- Pour plus de détails sur l'API, reportez-vous GetCloudFrontOriginAccessIdentityConfigà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`GetDistribution`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetDistribution`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Commencez avec un réseau de distribution de contenu de base

CLI

AWS CLI

Pour obtenir une CloudFront distribution

L'`get-distribution`exemple suivant obtient la CloudFront distribution avec l'ID`EDFDVBD6EXAMPLE`, y compris son`ETag`. L'ID de distribution est renvoyé dans les commandes create-distribution et list-distributions.

```
aws cloudfront get-distribution \
    --id EDFDVBD6EXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "Deployed",
        "LastModifiedTime": "2019-12-04T23:35:41.433Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
```

```
        "DistributionConfig": {
            "CallerReference": "cli-example",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-
example",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
```

```
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
```

```
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous GetDistributionà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : extrait les informations d'une distribution spécifique.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Pour plus de détails sur l'API, reportez-vous GetDistributionà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : extrait les informations d'une distribution spécifique.

```
Get-CFDistribution -Id EXAMPLE0000ID
```

- Pour plus de détails sur l'API, reportez-vous GetDistributionà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`GetDistributionConfig`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `GetDistributionConfig`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Commencez avec un réseau de distribution de contenu de base

CLI

AWS CLI

Pour obtenir une configuration CloudFront de distribution

L'exemple suivant obtient les métadonnées relatives à la CloudFront distribution avec l'IDEDFDVBD6EXAMPLE, y compris sonETag. L'ID de distribution est renvoyé dans les commandes create-distribution et list-distributions.

```
aws cloudfront get-distribution-config \
    --id EDFDVBD6EXAMPLE
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "DistributionConfig": {
        "CallerReference": "cli-example",
        "Aliases": {
            "Quantity": 0
        },
        "DefaultRootObject": "index.html",
        "Origins": {
            "Quantity": 1,
            "Items": [
                {
                    "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
                    "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                    "OriginPath": "",
                    "CustomHeaders": {
                        "Quantity": 0
```

```
                    },
                    "S3OriginConfig": {
                        "OriginAccessIdentity": ""
                    }
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "amzn-s3-demo-bucket.s3.amazonaws.com-cli-example",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 0
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
                }
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
```

```
            "SmoothStreaming": false,
            "DefaultTTL": 86400,
            "MaxTTL": 31536000,
            "Compress": false,
            "LambdaFunctionAssociations": {
                "Quantity": 0
            },
            "FieldLevelEncryptionId": ""
        },
        "CacheBehaviors": {
            "Quantity": 0
        },
        "CustomErrorResponses": {
            "Quantity": 0
        },
        "Comment": "",
        "Logging": {
            "Enabled": false,
            "IncludeCookies": false,
            "Bucket": "",
            "Prefix": ""
        },
        "PriceClass": "PriceClass_All",
        "Enabled": true,
        "ViewerCertificate": {
            "CloudFrontDefaultCertificate": true,
            "MinimumProtocolVersion": "TLSv1",
            "CertificateSource": "cloudfront"
        },
        "Restrictions": {
            "GeoRestriction": {
                "RestrictionType": "none",
                "Quantity": 0
            }
        },
        "WebACLId": "",
        "HttpVersion": "http2",
        "IsIPV6Enabled": true
    }
}
```

- Pour plus de détails sur l'API, reportez-vous GetDistributionConfigà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : extrait la configuration d'une distribution spécifique.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Pour plus de détails sur l'API, reportez-vous GetDistributionConfigà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : extrait la configuration d'une distribution spécifique.

```
Get-CFDistributionConfig -Id EXAMPLE0000ID
```

- Pour plus de détails sur l'API, reportez-vous GetDistributionConfigà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class CloudFrontWrapper:
    """Encapsulates Amazon CloudFront operations."""

    def __init__(self, cloudfront_client):
        """
        :param cloudfront_client: A Boto3 CloudFront client
        """
        self.cloudfront_client = cloudfront_client
```

```
    def update_distribution(self):
        distribution_id = input(
            "This script updates the comment for a CloudFront distribution.\n"
            "Enter a CloudFront distribution ID: "
        )

        distribution_config_response =
self.cloudfront_client.get_distribution_config(
            Id=distribution_id
        )
        distribution_config = distribution_config_response["DistributionConfig"]
        distribution_etag = distribution_config_response["ETag"]

        distribution_config["Comment"] = input(
            f"\nThe current comment for distribution {distribution_id} is "
            f"'{distribution_config['Comment']}'.\n"
            f"Enter a new comment: "
        )
        self.cloudfront_client.update_distribution(
            DistributionConfig=distribution_config,
            Id=distribution_id,
            IfMatch=distribution_etag,
        )
        print("Done!")
```

- Pour plus de détails sur l'API, consultez GetDistributionConfigle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **`ListCloudFrontOriginAccessIdentities`** avec une CLI

Les exemples de code suivants illustrent comment utiliser `ListCloudFrontOriginAccessIdentities`.

CLI

AWS CLI

Pour répertorier les identités CloudFront d'accès à l'origine

L'exemple suivant permet d'obtenir une liste des identités CloudFront d'accès à l'origine (OAI) de votre AWS compte :

```
aws cloudfront list-cloud-front-origin-access-identities
```

Sortie :

```
{
    "CloudFrontOriginAccessIdentityList": {
        "Items": [
            {
                "Id": "E74FTE3AEXAMPLE",
                "S3CanonicalUserId":
 "cd13868f797c227fbea2830611a26fe0a21ba1b826ab4bed9b7771c9aEXAMPLE",
                "Comment": "Example OAI"
            },
            {
                "Id": "EH1HDMBEXAMPLE",
                "S3CanonicalUserId":
 "1489f6f2e6faacaae7ff64c4c3e6956c24f78788abfc1718c3527c263bf7a17EXAMPLE",
                "Comment": "Test OAI"
            },
            {
                "Id": "E2X2C9TEXAMPLE",
                "S3CanonicalUserId":
 "cbfeebb915a64749f9be546a45b3fcfd3a31c779673c13c4dd460911ae402c2EXAMPLE",
                "Comment": "Example OAI #2"
            }
        ]
    }
}
```

- Pour plus de détails sur l'API, reportez-vous ListCloudFrontOriginAccessIdentitiesà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cet exemple renvoie une liste des identités CloudFront d'accès d'origine Amazon. Comme le MaxItem paramètre - spécifie une valeur de 2, les résultats incluent deux identités.

```
Get-CFCloudFrontOriginAccessIdentityList -MaxItem 2
```

Sortie :

```
IsTruncated : True
Items       : {E326XXXXXXXXXT, E1YWXXXXXXX9B}
Marker      :
MaxItems    : 2
NextMarker  : E1YXXXXXXXXX9B
Quantity    : 2
```

- Pour plus de détails sur l'API, reportez-vous ListCloudFrontOriginAccessIdentitiesà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cet exemple renvoie une liste des identités CloudFront d'accès d'origine Amazon. Comme le MaxItem paramètre - spécifie une valeur de 2, les résultats incluent deux identités.

```
Get-CFCloudFrontOriginAccessIdentityList -MaxItem 2
```

Sortie :

```
IsTruncated : True
Items       : {E326XXXXXXXXXT, E1YWXXXXXXX9B}
Marker      :
MaxItems    : 2
NextMarker  : E1YXXXXXXXXX9B
Quantity    : 2
```

- Pour plus de détails sur l'API, reportez-vous ListCloudFrontOriginAccessIdentitiesà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`ListDistributions`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `ListDistributions`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Commencer à utiliser les pare-feux pour applications Web

CLI

AWS CLI

Pour répertorier CloudFront les distributions

L'exemple suivant permet d'obtenir la liste des CloudFront distributions de votre AWS compte.

```
aws cloudfront list-distributions
```

Sortie :

```
{
    "DistributionList": {
        "Items": [
            {
                "Id": "E23YS8OEXAMPLE",
                "ARN": "arn:aws:cloudfront::123456789012:distribution/
E23YS8OEXAMPLE",
                "Status": "Deployed",
                "LastModifiedTime": "2024-08-05T18:23:40.375000+00:00",
                "DomainName": "abcdefgh12ijk.cloudfront.net",
                "Aliases": {
                    "Quantity": 0
                },
                "Origins": {
                    "Quantity": 1,
                    "Items": [
```

```
                        {
                            "Id": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                            "DomainName": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                            "OriginPath": "",
                            "CustomHeaders": {
                                "Quantity": 0
                            },
                            "S3OriginConfig": {
                                "OriginAccessIdentity": ""
                            },
                            "ConnectionAttempts": 3,
                            "ConnectionTimeout": 10,
                            "OriginShield": {
                                "Enabled": false
                            },
                            "OriginAccessControlId": "EIAP8PEXAMPLE"
                        }
                    ]
                },
                "OriginGroups": {
                    "Quantity": 0
                },
                "DefaultCacheBehavior": {
                    "TargetOriginId": "amzn-s3-demo-bucket.s3.us-
east-1.amazonaws.com",
                    "TrustedSigners": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "TrustedKeyGroups": {
                        "Enabled": false,
                        "Quantity": 0
                    },
                    "ViewerProtocolPolicy": "allow-all",
                    "AllowedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ],
                        "CachedMethods": {
                            "Quantity": 2,
```

```
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "Compress": true,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": "",
                "CachePolicyId": "658327ea-f89d-4fab-a63d-7e886EXAMPLE"
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "SSLSupportMethod": "vip",
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "HTTP2",
            "IsIPV6Enabled": true,
            "Staging": false
        }
    ]
```

```
    }
}
```

- Pour plus de détails sur l'API, reportez-vous ListDistributionsà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : renvoie les distributions.

```
Get-CFDistributionList
```

- Pour plus de détails sur l'API, reportez-vous ListDistributionsà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : renvoie les distributions.

```
Get-CFDistributionList
```

- Pour plus de détails sur l'API, reportez-vous ListDistributionsà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class CloudFrontWrapper:
    """Encapsulates Amazon CloudFront operations."""
```

```
    def __init__(self, cloudfront_client):
        """
        :param cloudfront_client: A Boto3 CloudFront client
        """
        self.cloudfront_client = cloudfront_client


    def list_distributions(self):
        print("CloudFront distributions:\n")
        distributions = self.cloudfront_client.list_distributions()
        if distributions["DistributionList"]["Quantity"] > 0:
            for distribution in distributions["DistributionList"]["Items"]:
                print(f"Domain: {distribution['DomainName']}")
                print(f"Distribution Id: {distribution['Id']}")
                print(
                    f"Certificate Source: "
                    f"{distribution['ViewerCertificate']['CertificateSource']}"
                )
                if distribution["ViewerCertificate"]["CertificateSource"] ==
 "acm":
                    print(
                        f"Certificate: {distribution['ViewerCertificate']
['Certificate']}"
                    )
                print("")
        else:
            print("No CloudFront distributions detected.")
```

- Pour plus de détails sur l'API, consultez ListDistributionsle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        oo_result = lo_fnt->listdistributions( ). " oo_result is returned for
testing purposes. "
        MESSAGE 'Retrieved list of CloudFront distributions.' TYPE 'I'.
      CATCH /aws1/cx_fntinvalidargument.
        MESSAGE 'Invalid argument provided.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous ListDistributionsà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **`UpdateDistribution`**avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser `UpdateDistribution`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Commencez avec un réseau de distribution de contenu de base

CLI

AWS CLI

Exemple 1 : pour mettre à jour l'objet racine par défaut d'une CloudFront distribution

L'exemple suivant met à jour l'objet racine par défaut `index.html` pour la CloudFront distribution avec l'`IDEDFDVBD6EXAMPLE`.

```
aws cloudfront update-distribution \
    --id EDFDVBD6EXAMPLE \
    --default-root-object index.html
```

Sortie :

```
{
    "ETag": "E2QWRUHEXAMPLE",
    "Distribution": {
        "Id": "EDFDVBD6EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EDFDVBD6EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-06T18:55:39.870Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "6b10378d-49be-4c4b-a642-419ccaf8f3b5",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "example-website",
                        "DomainName": "www.example.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "CustomOriginConfig": {
                            "HTTPPort": 80,
                            "HTTPSPort": 443,
                            "OriginProtocolPolicy": "match-viewer",
                            "OriginSslProtocols": {
                                "Quantity": 2,
                                "Items": [
                                    "SSLv3",
                                    "TLSv1"
                                ]
                            },
                            "OriginReadTimeout": 30,
                            "OriginKeepaliveTimeout": 5
                        }
```

```
                }
            ]
        },
        "OriginGroups": {
            "Quantity": 0
        },
        "DefaultCacheBehavior": {
            "TargetOriginId": "example-website",
            "ForwardedValues": {
                "QueryString": false,
                "Cookies": {
                    "Forward": "none"
                },
                "Headers": {
                    "Quantity": 1,
                    "Items": [
                        "*"
                    ]
                },
                "QueryStringCacheKeys": {
                    "Quantity": 0
                }
            },
            "TrustedSigners": {
                "Enabled": false,
                "Quantity": 0
            },
            "ViewerProtocolPolicy": "allow-all",
            "MinTTL": 0,
            "AllowedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ],
                "CachedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ]
                }
            },
            "SmoothStreaming": false,
```

```
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": true,
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http1.1",
            "IsIPV6Enabled": true
        }
    }
}
```

Exemple 2 : pour mettre à jour une CloudFront distribution

L'exemple suivant désactive la CloudFront distribution avec l'ID `EMLARXS9EXAMPLE` en fournissant la configuration de distribution dans un fichier JSON nommé`dist-config-disable.json`. Pour mettre à jour une distribution, vous devez utiliser l'option `--if-match` permettant de fournir l'`ETag` de la distribution. Pour l'obtenir l'`ETag`, utilisez la commande get-distribution ou get-distribution-config. Notez que le champ `Enabled` est défini sur `false` dans le fichier JSON.

Après avoir utilisé l'exemple suivant pour désactiver une distribution, vous pouvez utiliser la commande delete-distribution pour la supprimer.

```
aws cloudfront update-distribution \
    --id EMLARXS9EXAMPLE \
    --if-match E2QWRUHEXAMPLE \
    --distribution-config file://dist-config-disable.json
```

Contenu de `dist-config-disable.json` :

```
{
    "CallerReference": "cli-1574382155-496510",
    "Aliases": {
        "Quantity": 0
    },
    "DefaultRootObject": "index.html",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "amzn-s3-demo-bucket.s3.amazonaws.com-1574382155-273939",
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "OriginPath": "",
                "CustomHeaders": {
                    "Quantity": 0
                },
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                }
            }
        ]
    },
    "OriginGroups": {
        "Quantity": 0
    },
```

```
    "DefaultCacheBehavior": {
        "TargetOriginId": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            },
            "Headers": {
                "Quantity": 0
            },
            "QueryStringCacheKeys": {
                "Quantity": 0
            }
        },
        "TrustedSigners": {
            "Enabled": false,
            "Quantity": 0
        },
        "ViewerProtocolPolicy": "allow-all",
        "MinTTL": 0,
        "AllowedMethods": {
            "Quantity": 2,
            "Items": [
                "HEAD",
                "GET"
            ],
            "CachedMethods": {
                "Quantity": 2,
                "Items": [
                    "HEAD",
                    "GET"
                ]
            }
        },
        "SmoothStreaming": false,
        "DefaultTTL": 86400,
        "MaxTTL": 31536000,
        "Compress": false,
        "LambdaFunctionAssociations": {
            "Quantity": 0
        },
        "FieldLevelEncryptionId": ""
    },
```

```
    "CacheBehaviors": {
        "Quantity": 0
    },
    "CustomErrorResponses": {
        "Quantity": 0
    },
    "Comment": "",
    "Logging": {
        "Enabled": false,
        "IncludeCookies": false,
        "Bucket": "",
        "Prefix": ""
    },
    "PriceClass": "PriceClass_All",
    "Enabled": false,
    "ViewerCertificate": {
        "CloudFrontDefaultCertificate": true,
        "MinimumProtocolVersion": "TLSv1",
        "CertificateSource": "cloudfront"
    },
    "Restrictions": {
        "GeoRestriction": {
            "RestrictionType": "none",
            "Quantity": 0
        }
    },
    "WebACLId": "",
    "HttpVersion": "http2",
    "IsIPV6Enabled": true
}
```

Sortie :

```
{
    "ETag": "E9LHASXEXAMPLE",
    "Distribution": {
        "Id": "EMLARXS9EXAMPLE",
        "ARN": "arn:aws:cloudfront::123456789012:distribution/EMLARXS9EXAMPLE",
        "Status": "InProgress",
        "LastModifiedTime": "2019-12-06T18:32:35.553Z",
        "InProgressInvalidationBatches": 0,
        "DomainName": "d111111abcdef8.cloudfront.net",
        "ActiveTrustedSigners": {
```

```
            "Enabled": false,
            "Quantity": 0
        },
        "DistributionConfig": {
            "CallerReference": "cli-1574382155-496510",
            "Aliases": {
                "Quantity": 0
            },
            "DefaultRootObject": "index.html",
            "Origins": {
                "Quantity": 1,
                "Items": [
                    {
                        "Id": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
                        "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                        "OriginPath": "",
                        "CustomHeaders": {
                            "Quantity": 0
                        },
                        "S3OriginConfig": {
                            "OriginAccessIdentity": ""
                        }
                    }
                ]
            },
            "OriginGroups": {
                "Quantity": 0
            },
            "DefaultCacheBehavior": {
                "TargetOriginId": "amzn-s3-demo-
bucket.s3.amazonaws.com-1574382155-273939",
                "ForwardedValues": {
                    "QueryString": false,
                    "Cookies": {
                        "Forward": "none"
                    },
                    "Headers": {
                        "Quantity": 0
                    },
                    "QueryStringCacheKeys": {
                        "Quantity": 0
                    }
                },
```

```
                "TrustedSigners": {
                    "Enabled": false,
                    "Quantity": 0
                },
                "ViewerProtocolPolicy": "allow-all",
                "MinTTL": 0,
                "AllowedMethods": {
                    "Quantity": 2,
                    "Items": [
                        "HEAD",
                        "GET"
                    ],
                    "CachedMethods": {
                        "Quantity": 2,
                        "Items": [
                            "HEAD",
                            "GET"
                        ]
                    }
                },
                "SmoothStreaming": false,
                "DefaultTTL": 86400,
                "MaxTTL": 31536000,
                "Compress": false,
                "LambdaFunctionAssociations": {
                    "Quantity": 0
                },
                "FieldLevelEncryptionId": ""
            },
            "CacheBehaviors": {
                "Quantity": 0
            },
            "CustomErrorResponses": {
                "Quantity": 0
            },
            "Comment": "",
            "Logging": {
                "Enabled": false,
                "IncludeCookies": false,
                "Bucket": "",
                "Prefix": ""
            },
            "PriceClass": "PriceClass_All",
            "Enabled": false,
```

```
            "ViewerCertificate": {
                "CloudFrontDefaultCertificate": true,
                "MinimumProtocolVersion": "TLSv1",
                "CertificateSource": "cloudfront"
            },
            "Restrictions": {
                "GeoRestriction": {
                    "RestrictionType": "none",
                    "Quantity": 0
                }
            },
            "WebACLId": "",
            "HttpVersion": "http2",
            "IsIPV6Enabled": true
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous UpdateDistributionà la section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionRequest;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.Distribution;
import software.amazon.awssdk.services.cloudfront.model.DistributionConfig;
import
 software.amazon.awssdk.services.cloudfront.model.UpdateDistributionRequest;
import software.amazon.awssdk.services.cloudfront.model.CloudFrontException;
```

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class ModifyDistribution {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <id>\s

                Where:
                    id - the id value of the distribution.\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String id = args[0];
        CloudFrontClient cloudFrontClient = CloudFrontClient.builder()
                .region(Region.AWS_GLOBAL)
                .build();

        modDistribution(cloudFrontClient, id);
        cloudFrontClient.close();
    }

    public static void modDistribution(CloudFrontClient cloudFrontClient, String
 idVal) {
        try {
            // Get the Distribution to modify.
            GetDistributionRequest disRequest = GetDistributionRequest.builder()
                    .id(idVal)
                    .build();

            GetDistributionResponse response =
 cloudFrontClient.getDistribution(disRequest);
```

```
            Distribution disObject = response.distribution();
            DistributionConfig config = disObject.distributionConfig();

            // Create a new DistributionConfig object and add new values to
 comment and
            // aliases
            DistributionConfig config1 = DistributionConfig.builder()
                    .aliases(config.aliases()) // You can pass in new values here
                    .comment("New Comment")
                    .cacheBehaviors(config.cacheBehaviors())
                    .priceClass(config.priceClass())
                    .defaultCacheBehavior(config.defaultCacheBehavior())
                    .enabled(config.enabled())
                    .callerReference(config.callerReference())
                    .logging(config.logging())
                    .originGroups(config.originGroups())
                    .origins(config.origins())
                    .restrictions(config.restrictions())
                    .defaultRootObject(config.defaultRootObject())
                    .webACLId(config.webACLId())
                    .httpVersion(config.httpVersion())
                    .viewerCertificate(config.viewerCertificate())
                    .customErrorResponses(config.customErrorResponses())
                    .build();

            UpdateDistributionRequest updateDistributionRequest =
 UpdateDistributionRequest.builder()
                    .distributionConfig(config1)
                    .id(disObject.id())
                    .ifMatch(response.eTag())
                    .build();

            cloudFrontClient.updateDistribution(updateDistributionRequest);

        } catch (CloudFrontException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous UpdateDistributionà la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class CloudFrontWrapper:
    """Encapsulates Amazon CloudFront operations."""

    def __init__(self, cloudfront_client):
        """
        :param cloudfront_client: A Boto3 CloudFront client
        """
        self.cloudfront_client = cloudfront_client


    def update_distribution(self):
        distribution_id = input(
            "This script updates the comment for a CloudFront distribution.\n"
            "Enter a CloudFront distribution ID: "
        )

        distribution_config_response =
 self.cloudfront_client.get_distribution_config(
            Id=distribution_id
        )
        distribution_config = distribution_config_response["DistributionConfig"]
        distribution_etag = distribution_config_response["ETag"]

        distribution_config["Comment"] = input(
            f"\nThe current comment for distribution {distribution_id} is "
            f"'{distribution_config['Comment']}'.\n"
            f"Enter a new comment: "
        )
```

```
        self.cloudfront_client.update_distribution(
            DistributionConfig=distribution_config,
            Id=distribution_id,
            IfMatch=distribution_etag,
        )
        print("Done!")
```

- Pour plus de détails sur l'API, consultez UpdateDistributionle AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        " Get the current distribution configuration and ETag "
        DATA(lo_distribution_config_result) = lo_fnt-
>getdistributionconfig( iv_id = iv_distribution_id ).
        DATA(lo_old_config) = lo_distribution_config_result-
>get_distributionconfig( ).
        DATA(lv_etag) = lo_distribution_config_result->get_etag( ).

        " Create a new distribution config with the updated comment "
        " Since the config object is immutable, we need to create a new one with
 all existing values "
        DATA(lo_new_config) = NEW /aws1/cl_fntdistributionconfig(
          iv_callerreference = lo_old_config->get_callerreference( )
          io_aliases = lo_old_config->get_aliases( )
          iv_defaultrootobject = lo_old_config->get_defaultrootobject( )
          io_origins = lo_old_config->get_origins( )
          io_origingroups = lo_old_config->get_origingroups( )
          io_defaultcachebehavior = lo_old_config->get_defaultcachebehavior( )
```

```
          io_cachebehaviors = lo_old_config->get_cachebehaviors( )
          io_customerrorresponses = lo_old_config->get_customerrorresponses( )
          iv_comment = iv_comment
          io_logging = lo_old_config->get_logging( )
          iv_priceclass = lo_old_config->get_priceclass( )
          iv_enabled = lo_old_config->get_enabled( )
          io_viewercertificate = lo_old_config->get_viewercertificate( )
          io_restrictions = lo_old_config->get_restrictions( )
          iv_webaclid = lo_old_config->get_webaclid( )
          iv_httpversion = lo_old_config->get_httpversion( )
          iv_isipv6enabled = lo_old_config->get_isipv6enabled( ) ).

        " Update the distribution with the modified configuration "
        lo_fnt->updatedistribution(
          io_distributionconfig = lo_new_config
          iv_id = iv_distribution_id
          iv_ifmatch = lv_etag ).
        MESSAGE 'CloudFront distribution updated successfully.' TYPE 'I'.
      CATCH /aws1/cx_fntnosuchdistribution.
        MESSAGE 'Distribution does not exist.' TYPE 'E'.
      CATCH /aws1/cx_fntpreconditionfailed.
        MESSAGE 'Precondition failed - ETag mismatch.' TYPE 'E'.
      CATCH /aws1/cx_fntinvalidifmatchvrs.
        MESSAGE 'Invalid If-Match version.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous UpdateDistributionà la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Scénarios d' CloudFront utilisation AWS Kits SDK

Les exemples de code suivants vous montrent comment implémenter des scénarios courants CloudFront avec AWS les SDK. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein de celles-ci CloudFront ou en les combinant avec d'autres Services AWS. Chaque exemple inclut un lien vers le code source complet, où vous trouverez des instructions sur la configuration et l’exécution du code.

Les scénarios ciblent un niveau d'expérience intermédiaire pour vous aider à comprendre les actions de service dans leur contexte.

Exemples

- Créez des ressources pour les gestionnaires SaaS AWS Kit SDK
- Supprimer les ressources CloudFront de signature à l'aide de AWS Kit SDK
- Commencez avec un réseau de distribution de contenu de base
- Commencer à utiliser les pare-feux pour applications Web
- Créez des URL signées et des cookies à l'aide d'un AWS Kit SDK

Créez des ressources pour les gestionnaires SaaS AWS Kit SDK

L'exemple de code suivant montre comment créer une distribution à locataires multiples et un locataire de distribution avec différentes configurations.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

L'exemple suivant montre comment créer une distribution à locataires multiples à l'aide de paramètres et d'un certificat générique.

```
import software.amazon.awssdk.core.internal.waiters.ResponseOrException;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.ConnectionMode;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.Distribution;
import software.amazon.awssdk.services.cloudfront.model.GetDistributionResponse;
import software.amazon.awssdk.services.cloudfront.model.HttpVersion;
import software.amazon.awssdk.services.cloudfront.model.Method;
import software.amazon.awssdk.services.cloudfront.model.SSLSupportMethod;
```

```
import software.amazon.awssdk.services.cloudfront.model.ViewerProtocolPolicy;
import software.amazon.awssdk.services.cloudfront.waiters.CloudFrontWaiter;
import software.amazon.awssdk.services.s3.S3Client;

import java.time.Instant;

public class CreateMultiTenantDistribution {
    public static Distribution
 CreateMultiTenantDistributionWithCert(CloudFrontClient cloudFrontClient,
                                                                    S3Client
 s3Client,
                                                                    final String
 bucketName,
                                                                    final String
 certificateArn) {
        // fetch the origin info if necessary
        final String region = s3Client.headBucket(b ->
 b.bucket(bucketName)).sdkHttpResponse().headers()
                .get("x-amz-bucket-region").get(0);
        final String originDomain = bucketName + ".s3." + region +
 ".amazonaws.com";
        String originId = originDomain; // Use the originDomain value for the
 originId.

        CreateDistributionResponse createDistResponse =
 cloudFrontClient.createDistribution(builder -> builder
                .distributionConfig(b1 -> b1
                        .httpVersion(HttpVersion.HTTP2)
                        .enabled(true)
                        .comment("Template Distribution with cert built with
 java")
                        .connectionMode(ConnectionMode.TENANT_ONLY)
                        .callerReference(Instant.now().toString())
                        .viewerCertificate(certBuilder -> certBuilder
                                .acmCertificateArn(certificateArn)
                                .sslSupportMethod(SSLSupportMethod.SNI_ONLY))
                        .origins(b2 -> b2
                                .quantity(1)
                                .items(b3 -> b3
                                        .domainName(originDomain)
                                        .id(originId)
                                        .originPath("/{{tenantName}}")
                                        .s3OriginConfig(builder4 -> builder4
                                                .originAccessIdentity(
```

```
                                                        ""))))
                        .tenantConfig(b5 -> b5
                                .parameterDefinitions(b6 -> b6
                                        .name("tenantName")
                                        .definition(b7 -> b7
                                                .stringSchema(b8 -> b8
                                                        .comment("tenantName
 value")
                                                        .defaultValue("root")
                                                        .required(false)))))
                        .defaultCacheBehavior(b2 -> b2

 .viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)
                                .targetOriginId(originId)
                                .cachePolicyId("658327ea-f89d-4fab-
a63d-7e88639e58f6") // CachingOptimized Policy
                                .allowedMethods(b4 -> b4
                                        .quantity(2)
                                        .items(Method.HEAD, Method.GET)))
                ));

        final Distribution distribution = createDistResponse.distribution();
        try (CloudFrontWaiter cfWaiter =
 CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
            ResponseOrException<GetDistributionResponse> responseOrException =
 cfWaiter
                    .waitUntilDistributionDeployed(builder ->
 builder.id(distribution.id()))
                    .matched();
            responseOrException.response()
                    .orElseThrow(() -> new RuntimeException("Distribution not
 created"));
        }
        return distribution;
    }

    public static Distribution
 CreateMultiTenantDistributionNoCert(CloudFrontClient cloudFrontClient,
                                                                S3Client s3Client,
                                                                final String
 bucketName) {
        // fetch the origin info if necessary
        final String region = s3Client.headBucket(b ->
 b.bucket(bucketName)).sdkHttpResponse().headers()
```

```
                .get("x-amz-bucket-region").get(0);
        final String originDomain = bucketName + ".s3." + region +
 ".amazonaws.com";
        String originId = originDomain; // Use the originDomain value for the
 originId.

        CreateDistributionResponse createDistResponse =
 cloudFrontClient.createDistribution(builder -> builder
                .distributionConfig(b1 -> b1
                        .httpVersion(HttpVersion.HTTP2)
                        .enabled(true)
                        .comment("Template Distribution with cert built with
 java")
                        .connectionMode(ConnectionMode.TENANT_ONLY)
                        .callerReference(Instant.now().toString())
                        .origins(b2 -> b2
                                .quantity(1)
                                .items(b3 -> b3
                                        .domainName(originDomain)
                                        .id(originId)
                                        .originPath("/{{tenantName}}")
                                        .s3OriginConfig(builder4 -> builder4
                                                .originAccessIdentity(
                                                        ""))))
                        .tenantConfig(b5 -> b5
                                .parameterDefinitions(b6 -> b6
                                        .name("tenantName")
                                        .definition(b7 -> b7
                                                .stringSchema(b8 -> b8
                                                        .comment("tenantName
 value")
                                                        .defaultValue("root")
                                                        .required(false)))))
                        .defaultCacheBehavior(b2 -> b2

 .viewerProtocolPolicy(ViewerProtocolPolicy.ALLOW_ALL)
                                .targetOriginId(originId)
                                .cachePolicyId("658327ea-f89d-4fab-
a63d-7e88639e58f6") // CachingOptimized Policy
                                .allowedMethods(b4 -> b4
                                        .quantity(2)
                                        .items(Method.HEAD, Method.GET)))
                ));
```

```
        final Distribution distribution = createDistResponse.distribution();
        try (CloudFrontWaiter cfWaiter =
 CloudFrontWaiter.builder().client(cloudFrontClient).build()) {
            ResponseOrException<GetDistributionResponse> responseOrException =
 cfWaiter
                    .waitUntilDistributionDeployed(builder ->
 builder.id(distribution.id()))
                    .matched();
            responseOrException.response()
                    .orElseThrow(() -> new RuntimeException("Distribution not
 created"));
        }
        return distribution;
    }
}
```

L’exemple suivant montre comment créer un locataire de distribution associé à ce modèle, notamment en utilisant le paramètre déclaré ci-dessus. Notez qu’il n’est pas nécessaire d’ajouter des informations de certificat ici, car notre domaine est déjà couvert par le modèle parent.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantNoCert(CloudFrontClient cloudFrontClient,
                                                                    Route53Client
 route53Client,
```

```
                                                                    String
distributionId,
                                                                    String
domain,
                                                                    String
hostedZoneId) {
        CreateDistributionTenantResponse createResponse =
cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .enabled(false)
                .name("no-cert-tenant")
        );

        final DistributionTenant distributionTenant =
createResponse.distributionTenant();

        // Then update the Route53 hosted zone to point your domain at the
distribution tenant
        // We fetch the RoutingEndpoint to point to via the default connection
group that was created for your tenant
        final GetConnectionGroupResponse fetchedConnectionGroup =
cloudFrontClient.getConnectionGroup(builder -> builder
                .identifier(distributionTenant.connectionGroupId()));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("ChangeBatch comment")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type("CNAME")
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

.value(fetchedConnectionGroup.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));
        return distributionTenant;
```

```
    }

}
```

Si le certificat de visualisation a été omis dans le modèle parent, vous devez plutôt ajouter des informations de certificat sur le ou les locataires qui lui sont associés. L'exemple suivant montre comment procéder via un ARN de certificat ACM qui couvre le domaine nécessaire pour le locataire.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantWithCert(CloudFrontClient cloudFrontClient,

 Route53Client route53Client,
                                                                    String
 distributionId,
                                                                    String
 domain,
                                                                    String
 hostedZoneId,
                                                                    String
 certificateArn) {
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
```

```
                        .domain(domain))
                .enabled(false)
                .name("tenant-with-cert")
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .customizations(b3 -> b3
                        .certificate(b4 -> b4
                                .arn(certificateArn))) // NOTE: Cert must be in
Us-East-1 and cover the domain provided in this request

        );

        final DistributionTenant distributionTenant =
createResponse.distributionTenant();

        // Then update the Route53 hosted zone to point your domain at the
distribution tenant
        // We fetch the RoutingEndpoint to point to via the default connection
group that was created for your tenant
        final GetConnectionGroupResponse fetchedConnectionGroup =
cloudFrontClient.getConnectionGroup(builder -> builder
                .identifier(distributionTenant.connectionGroupId()));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
                        .comment("ChangeBatch comment")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type("CNAME")
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

.value(fetchedConnectionGroup.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));
        return distributionTenant;
    }

}
```

L'exemple suivant montre comment procéder avec une demande de certificat CloudFront-hosted gérée. Cette option est idéale si vous n'avez pas déjà du trafic vers votre domaine. Dans ce cas, nous créons un ConnectionGroup pour générer un RoutingEndpoint. Ensuite, nous l'utilisons RoutingEndpoint pour créer des enregistrements DNS qui vérifient la propriété du domaine et pointent vers CloudFront. CloudFront servira ensuite automatiquement un jeton pour valider la propriété du domaine et créer un certificat géré.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantCfHosted(CloudFrontClient cloudFrontClient,

 Route53Client route53Client,
                                                                    String
 distributionId,
                                                                    String
 domain,
                                                                    String
 hostedZoneId) throws InterruptedException {
        CreateConnectionGroupResponse createConnectionGroupResponse =
 cloudFrontClient.createConnectionGroup(builder -> builder
                .ipv6Enabled(true)
                .name("cf-hosted-connection-group")
                .enabled(true));

        route53Client.changeResourceRecordSets(builder -> builder
                .hostedZoneId(hostedZoneId)
                .changeBatch(b1 -> b1
```

```
                        .comment("cf-hosted domain validation record")
                        .changes(b2 -> b2
                                .resourceRecordSet(b3 -> b3
                                        .name(domain)
                                        .type(RRType.CNAME)
                                        .ttl(300L)
                                        .resourceRecords(b4 -> b4

.value(createConnectionGroupResponse.connectionGroup().routingEndpoint())))
                                .action("CREATE"))
                ));

        // Give the R53 record time to propagate, if it isn't being returned by
servers yet, the following call will fail
        Thread.sleep(60000);

        CreateDistributionTenantResponse createResponse =
cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))

.connectionGroupId(createConnectionGroupResponse.connectionGroup().id())
                .enabled(false)
                .name("cf-hosted-tenant")
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .managedCertificateRequest(b3 -> b3
                        .validationTokenHost(ValidationTokenHost.CLOUDFRONT)
                )
        );

        return createResponse.distributionTenant();
    }

}
```

L’exemple suivant montre comment procéder avec une demande de certificat géré auto-hébergée. Ceci est idéal si vous avez du trafic vers votre domaine et que vous ne pouvez pas tolérer les durées d’indisponibilité lors d’une migration. À la fin de cet exemple, le locataire sera créé dans un état en attente de validation du domaine et de configuration DNS. Suivez

les étapes [ici] (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/managed-cloudfront-certificates.html#complete -domain-ownership) pour terminer la configuration lorsque vous êtes prêt à migrer le trafic.

```
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import
 software.amazon.awssdk.services.cloudfront.model.CreateConnectionGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.CreateDistributionTenantResponse;
import software.amazon.awssdk.services.cloudfront.model.DistributionTenant;
import
 software.amazon.awssdk.services.cloudfront.model.GetConnectionGroupResponse;
import software.amazon.awssdk.services.cloudfront.model.ValidationTokenHost;
import software.amazon.awssdk.services.route53.Route53Client;
import software.amazon.awssdk.services.route53.model.RRType;

import java.time.Instant;

public class CreateDistributionTenant {

    public static DistributionTenant
 createDistributionTenantSelfHosted(CloudFrontClient cloudFrontClient,
                                                                    String
 distributionId,
                                                                    String
 domain) {
        CreateDistributionTenantResponse createResponse =
 cloudFrontClient.createDistributionTenant(builder -> builder
                .distributionId(distributionId)
                .domains(b1 -> b1
                        .domain(domain))
                .parameters(b2 -> b2
                        .name("tenantName")
                        .value("myTenant"))
                .enabled(false)
                .name("self-hosted-tenant")
                .managedCertificateRequest(b3 -> b3
                        .validationTokenHost(ValidationTokenHost.SELF_HOSTED)
                        .primaryDomainName(domain)
                )
        );
```

```
        return createResponse.distributionTenant();
    }

}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Java 2.x.
  - CreateDistribution
  - CreateDistributionTenant

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Supprimer les ressources CloudFront de signature à l'aide de AWS Kit SDK

L'exemple de code suivant montre comment supprimer des ressources utilisées pour accéder à un contenu restreint dans un compartiment Amazon Simple Storage Service (Amazon S3).

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontClient;
import software.amazon.awssdk.services.cloudfront.model.DeleteKeyGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.DeleteOriginAccessControlResponse;
import software.amazon.awssdk.services.cloudfront.model.DeletePublicKeyResponse;
import software.amazon.awssdk.services.cloudfront.model.GetKeyGroupResponse;
import
 software.amazon.awssdk.services.cloudfront.model.GetOriginAccessControlResponse;
```

```
import software.amazon.awssdk.services.cloudfront.model.GetPublicKeyResponse;

public class DeleteSigningResources {
    private static final Logger logger =
 LoggerFactory.getLogger(DeleteSigningResources.class);

    public static void deleteOriginAccessControl(final CloudFrontClient
 cloudFrontClient,
            final String originAccessControlId) {
        GetOriginAccessControlResponse getResponse = cloudFrontClient
                .getOriginAccessControl(b -> b.id(originAccessControlId));
        DeleteOriginAccessControlResponse deleteResponse =
 cloudFrontClient.deleteOriginAccessControl(builder -> builder
                .id(originAccessControlId)
                .ifMatch(getResponse.eTag()));
        if (deleteResponse.sdkHttpResponse().isSuccessful()) {
            logger.info("Successfully deleted Origin Access Control [{}]",
 originAccessControlId);
        }
    }

    public static void deleteKeyGroup(final CloudFrontClient cloudFrontClient,
 final String keyGroupId) {

        GetKeyGroupResponse getResponse = cloudFrontClient.getKeyGroup(b ->
 b.id(keyGroupId));
        DeleteKeyGroupResponse deleteResponse =
 cloudFrontClient.deleteKeyGroup(builder -> builder
                .id(keyGroupId)
                .ifMatch(getResponse.eTag()));
        if (deleteResponse.sdkHttpResponse().isSuccessful()) {
            logger.info("Successfully deleted Key Group [{}]", keyGroupId);
        }
    }

    public static void deletePublicKey(final CloudFrontClient cloudFrontClient,
 final String publicKeyId) {
        GetPublicKeyResponse getResponse = cloudFrontClient.getPublicKey(b ->
 b.id(publicKeyId));

        DeletePublicKeyResponse deleteResponse =
 cloudFrontClient.deletePublicKey(builder -> builder
                .id(publicKeyId)
                .ifMatch(getResponse.eTag()));
```

```
        if (deleteResponse.sdkHttpResponse().isSuccessful()) {
            logger.info("Successfully deleted Public Key [{}]", publicKeyId);
        }
    }
}
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Java 2.x.
  - DeleteKeyGroup
  - DeleteOriginAccessControl
  - DeletePublicKey

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Commencez avec un réseau de distribution de contenu de base

L'exemple de code suivant illustre comment :

- Créer un compartiment Amazon S3
- Importer du contenu dans le bucket
- Création d'une CloudFront distribution avec OAC
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code.

```
#!/bin/bash

# CloudFront Getting Started Tutorial Script
# This script creates an S3 bucket, uploads sample content, creates a CloudFront
 distribution with OAC,
# and demonstrates how to access content through CloudFront.

set -euo pipefail

# Set up logging
LOG_FILE="cloudfront-tutorial.log"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "Starting CloudFront Getting Started Tutorial at $(date)"

# Function to handle errors
handle_error() {
    echo "ERROR: $1" >&2
    echo "Resources created before error:"
    if [ -n "${BUCKET_NAME:-}" ]; then
        echo "- S3 Bucket: $BUCKET_NAME"
    fi
    if [ -n "${OAC_ID:-}" ]; then
        echo "- CloudFront Origin Access Control: $OAC_ID"
    fi
    if [ -n "${DISTRIBUTION_ID:-}" ]; then
        echo "- CloudFront Distribution: $DISTRIBUTION_ID"
    fi

    echo "Attempting to clean up resources..."
    cleanup
    exit 1
}

# Function to clean up resources
cleanup() {
    echo "Cleaning up resources..."

    if [ -n "${DISTRIBUTION_ID:-}" ]; then
        echo "Disabling CloudFront distribution $DISTRIBUTION_ID..."

        # Get the current configuration and ETag in one call
```

```
        DIST_CONFIG=$(aws cloudfront get-distribution-config --id
 "$DISTRIBUTION_ID" 2>/dev/null) || {
            echo "Failed to get distribution config. Continuing with cleanup..."
            DIST_CONFIG=""
        }

        if [ -n "$DIST_CONFIG" ]; then
            ETAG=$(echo "$DIST_CONFIG" | jq -r '.ETag')

            # Modify and update distribution in one pipeline
            if echo "$DIST_CONFIG" | jq '.DistributionConfig.Enabled = false' | \
                aws cloudfront update-distribution \
                    --id "$DISTRIBUTION_ID" \
                    --distribution-config "$(cat)" \
                    --if-match "$ETAG" 2>/dev/null; then

                echo "Waiting for distribution to be disabled (this may take
 several minutes)..."
                aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID"
 2>/dev/null || {
                    echo "Distribution deployment wait timed out. Proceeding with
 deletion..."
                }

                # Get fresh ETag for deletion
                DIST_CONFIG=$(aws cloudfront get-distribution-config --id
 "$DISTRIBUTION_ID" 2>/dev/null) || {
                    echo "Failed to get updated config. Skipping distribution
 deletion..."
                    DIST_CONFIG=""
                }

                if [ -n "$DIST_CONFIG" ]; then
                    ETAG=$(echo "$DIST_CONFIG" | jq -r '.ETag')
                    aws cloudfront delete-distribution --id "$DISTRIBUTION_ID" --
if-match "$ETAG" 2>/dev/null && \
                        echo "CloudFront distribution deleted." || \
                        echo "Failed to delete distribution. You may need to
 delete it manually."
                fi
            else
                echo "Failed to disable distribution. Continuing with cleanup..."
            fi
        fi
```

```
    fi

    if [ -n "${OAC_ID:-}" ]; then
        echo "Deleting Origin Access Control $OAC_ID..."
        OAC_DATA=$(aws cloudfront get-origin-access-control --id "$OAC_ID" 2>/
dev/null) || {
            echo "Failed to get Origin Access Control. You may need to delete it
 manually."
            OAC_DATA=""
        }

        if [ -n "$OAC_DATA" ]; then
            OAC_ETAG=$(echo "$OAC_DATA" | jq -r '.ETag')
            aws cloudfront delete-origin-access-control --id "$OAC_ID" --if-match
 "$OAC_ETAG" 2>/dev/null && \
                echo "Origin Access Control deleted." || \
                echo "Failed to delete Origin Access Control. You may need to
 delete it manually."
        fi
    fi

    if [ -n "${BUCKET_NAME:-}" ] && [ "$BUCKET_IS_SHARED" != "true" ]; then
        echo "Deleting S3 bucket $BUCKET_NAME and its contents..."
        aws s3 rm "s3://$BUCKET_NAME" --recursive 2>/dev/null || {
            echo "Failed to remove bucket contents. Continuing with bucket
 deletion..."
        }

        aws s3 rb "s3://$BUCKET_NAME" 2>/dev/null && \
            echo "S3 bucket deleted." || \
            echo "Failed to delete bucket. You may need to delete it manually."
    fi

    # Clean up temporary files
    rm -f temp_disabled_config.json distribution-config.json bucket-policy.json
 2>/dev/null || true
    rm -rf temp_content 2>/dev/null || true
}

# Trap errors and cleanup
trap 'handle_error "Script interrupted"' INT TERM

# Validate AWS CLI is available
if ! command -v aws &> /dev/null; then
```

```
    handle_error "AWS CLI is not installed or not in PATH"
fi

# Validate jq is available
if ! command -v jq &> /dev/null; then
    handle_error "jq is not installed or not in PATH"
fi

# Validate AWS credentials are configured
if ! aws sts get-caller-identity &> /dev/null; then
    handle_error "AWS credentials are not configured or invalid"
fi

# Initialize variables
BUCKET_NAME=""
OAC_ID=""
DISTRIBUTION_ID=""
BUCKET_IS_SHARED=false

# Generate a random identifier for the bucket name using secure random
RANDOM_ID=$(openssl rand -hex 6)
if [ -z "$RANDOM_ID" ]; then
    handle_error "Failed to generate random identifier"
fi

# Check for shared prereq bucket and get account ID in parallel calls
PREREQ_BUCKET=$(aws cloudformation describe-stacks --stack-name tutorial-prereqs-
bucket \
    --query 'Stacks[0].Outputs[?OutputKey==`BucketName`].OutputValue' --output
 text 2>/dev/null) || PREREQ_BUCKET=""

if [ -n "$PREREQ_BUCKET" ] && [ "$PREREQ_BUCKET" != "None" ]; then
    BUCKET_NAME="$PREREQ_BUCKET"
    BUCKET_IS_SHARED=true
    echo "Using shared bucket: $BUCKET_NAME"
else
    BUCKET_IS_SHARED=false
    BUCKET_NAME="cloudfront-${RANDOM_ID}"
fi
echo "Using bucket name: $BUCKET_NAME"

# Get AWS account ID early
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)
if [ $? -ne 0 ]; then
```

```
    handle_error "Failed to get AWS account ID"
fi

# Validate account ID format
if ! [[ "$ACCOUNT_ID" =~ ^[0-9]{12}$ ]]; then
    handle_error "Invalid AWS account ID format: $ACCOUNT_ID"
fi

# Create a temporary directory for content with restrictive permissions
TEMP_DIR="temp_content"
mkdir -p "$TEMP_DIR/css"
chmod 700 "$TEMP_DIR"
if [ $? -ne 0 ]; then
    handle_error "Failed to create temporary directory"
fi

# Step 1: Create an S3 bucket (only if not shared)
if [ "$BUCKET_IS_SHARED" != "true" ]; then
    echo "Creating S3 bucket: $BUCKET_NAME"
    aws s3 mb "s3://$BUCKET_NAME" --region us-east-1
    if [ $? -ne 0 ]; then
        handle_error "Failed to create S3 bucket"
    fi

    aws s3api put-bucket-tagging --bucket "$BUCKET_NAME" --tagging
 'TagSet=[{Key=project,Value=doc-smith},{Key=tutorial,Value=cloudfront-
gettingstarted}]'

    # Batch bucket configuration calls for efficiency
    aws s3api put-bucket-versioning --bucket "$BUCKET_NAME" --versioning-
configuration Status=Enabled &
    aws s3api put-public-access-block \
        --bucket "$BUCKET_NAME" \
        --public-access-block-configuration
 "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets
 &
    aws s3api put-bucket-encryption \
        --bucket "$BUCKET_NAME" \
        --server-side-encryption-configuration '{
            "Rules": [
                {
                    "ApplyServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "AES256"
                    }
```

```
                }
            ]
        }' &
    wait
fi

# Step 2: Create sample content
echo "Creating sample content..."
cat > "$TEMP_DIR/index.html" << 'EOF'
<!DOCTYPE html>
<html>
<head>
    <title>Hello World</title>
    <link rel="stylesheet" type="text/css" href="css/styles.css">
</head>
<body>
    <h1>Hello world!</h1>
</body>
</html>
EOF

cat > "$TEMP_DIR/css/styles.css" << 'EOF'
body {
    font-family: Arial, sans-serif;
    margin: 40px;
    background-color: #f5f5f5;
}
h1 {
    color: #333;
    text-align: center;
}
EOF

# Set restrictive permissions on content files
chmod 600 "$TEMP_DIR/index.html" "$TEMP_DIR/css/styles.css"

# Step 3: Upload content to the S3 bucket with encryption and metadata
echo "Uploading content to S3 bucket..."
aws s3 cp "$TEMP_DIR/" "s3://$BUCKET_NAME/" --recursive \
    --sse AES256 \
    --metadata "Source=CloudFrontTutorial"
if [ $? -ne 0 ]; then
    handle_error "Failed to upload content to S3 bucket"
fi
```

```
# Step 4: Create Origin Access Control
echo "Creating Origin Access Control..."
OAC_RESPONSE=$(aws cloudfront create-origin-access-control \
    --origin-access-control-config Name="oac-for-
$BUCKET_NAME",SigningProtocol=sigv4,SigningBehavior=always,OriginAccessControlOriginType=

if [ $? -ne 0 ]; then
    handle_error "Failed to create Origin Access Control"
fi

OAC_ID=$(echo "$OAC_RESPONSE" | jq -r '.OriginAccessControl.Id')
if [ -z "$OAC_ID" ] || [ "$OAC_ID" = "null" ]; then
    handle_error "Failed to extract OAC ID from response"
fi

# Validate OAC ID format (alphanumeric and hyphens)
if ! [[ "$OAC_ID" =~ ^[A-Z0-9]+$ ]]; then
    handle_error "Invalid OAC ID format: $OAC_ID"
fi

echo "Created Origin Access Control with ID: $OAC_ID"

# Step 5: Create CloudFront distribution
echo "Creating CloudFront distribution..."

# Validate bucket name format
if ! [[ "$BUCKET_NAME" =~ ^[a-z0-9][a-z0-9.-]*[a-z0-9]$ ]]; then
    handle_error "Invalid S3 bucket name format: $BUCKET_NAME"
fi

# Create distribution configuration with improved security settings
cat > distribution-config.json << EOF
{
    "CallerReference": "cli-tutorial-$(date +%s)",
    "Origins": {
        "Quantity": 1,
        "Items": [
            {
                "Id": "S3-$BUCKET_NAME",
                "DomainName": "$BUCKET_NAME.s3.amazonaws.com",
                "S3OriginConfig": {
                    "OriginAccessIdentity": ""
                },
```

```
                "OriginAccessControlId": "$OAC_ID"
            }
        ]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "S3-$BUCKET_NAME",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2,
            "Items": ["GET", "HEAD"],
            "CachedMethods": {
                "Quantity": 2,
                "Items": ["GET", "HEAD"]
            }
        },
        "DefaultTTL": 86400,
        "MinTTL": 0,
        "MaxTTL": 31536000,
        "Compress": true,
        "ForwardedValues": {
            "QueryString": false,
            "Cookies": {
                "Forward": "none"
            }
        }
    },
    "Comment": "CloudFront distribution for tutorial",
    "Enabled": true,
    "WebACLId": "",
    "HttpVersion": "http2and3"
}
EOF

# Set restrictive permissions on config file before passing credentials
chmod 600 distribution-config.json

DIST_RESPONSE=$(aws cloudfront create-distribution --distribution-config file://
distribution-config.json)
if [ $? -ne 0 ]; then
    handle_error "Failed to create CloudFront distribution"
fi

DISTRIBUTION_ID=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.Id')
DOMAIN_NAME=$(echo "$DIST_RESPONSE" | jq -r '.Distribution.DomainName')
```

```
if [ -z "$DISTRIBUTION_ID" ] || [ "$DISTRIBUTION_ID" = "null" ] || [ -z
 "$DOMAIN_NAME" ] || [ "$DOMAIN_NAME" = "null" ]; then
    handle_error "Failed to extract distribution ID or domain name from response"
fi

# Validate distribution ID format
if ! [[ "$DISTRIBUTION_ID" =~ ^[A-Z0-9]+$ ]]; then
    handle_error "Invalid distribution ID format: $DISTRIBUTION_ID"
fi

echo "Created CloudFront distribution with ID: $DISTRIBUTION_ID"
echo "CloudFront domain name: $DOMAIN_NAME"

# Tag the CloudFront distribution
aws cloudfront tag-resource --resource "arn:aws:cloudfront::
$ACCOUNT_ID:distribution/$DISTRIBUTION_ID" --tags 'Items=[{Key=project,Value=doc-
smith},{Key=tutorial,Value=cloudfront-gettingstarted}]'

# Step 6: Update S3 bucket policy
echo "Updating S3 bucket policy..."

cat > bucket-policy.json << EOF
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFrontServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudfront.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::$BUCKET_NAME/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudfront::
$ACCOUNT_ID:distribution/$DISTRIBUTION_ID"
                }
            }
        }
    ]
}
EOF
```

```
# Set restrictive permissions on policy file
chmod 600 bucket-policy.json

aws s3api put-bucket-policy --bucket "$BUCKET_NAME" --policy file://bucket-
policy.json
if [ $? -ne 0 ]; then
    handle_error "Failed to update S3 bucket policy"
fi

# Step 7: Wait for distribution to deploy
echo "Waiting for CloudFront distribution to deploy (this may take 5-10
 minutes)..."
aws cloudfront wait distribution-deployed --id "$DISTRIBUTION_ID" 2>/dev/null ||
 {
    echo "Warning: Distribution deployment wait timed out. The distribution may
 still be deploying."
}

echo "CloudFront distribution is now deployed."

# Step 8: Display access information
echo ""
echo "===== CloudFront Distribution Setup Complete ====="
echo "You can access your content at: https://$DOMAIN_NAME/index.html"
echo ""
echo "Resources created:"
echo "- S3 Bucket: $BUCKET_NAME"
echo "- CloudFront Origin Access Control: $OAC_ID"
echo "- CloudFront Distribution: $DISTRIBUTION_ID"
echo ""
echo "To clean up resources, run: cleanup"
echo ""

echo "Tutorial completed at $(date)"
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI.
  - CreateDistribution
  - CreateOriginAccessControl
  - DeleteDistribution
  - DeleteOriginAccessControl

- GetDistribution
- GetDistributionConfig
- GetOriginAccessControl
- UpdateDistribution
- WaitDistributionDeployed

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Commencer à utiliser les pare-feux pour applications Web

L'exemple de code suivant illustre comment :

- Création d'une liste ACL web
- Ajouter une règle de correspondance de chaînes
- Ajouter des règles gérées
- Configurer la journalisation
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code.

```
#!/bin/bash

# AWS WAF Getting Started Script
# This script creates a Web ACL with a string match rule and AWS Managed Rules,
# associates it with a CloudFront distribution, and then cleans up all resources.

set -euo pipefail
```

```
# Security: Restrict file permissions
umask 077

# Set up logging with secure file handling
LOG_FILE="waf-tutorial.log"
touch "$LOG_FILE"
chmod 600 "$LOG_FILE"
exec > >(tee -a "$LOG_FILE") 2>&1

echo "================================================="
echo "AWS WAF Getting Started Tutorial"
echo "================================================="
echo "This script will create AWS WAF resources and associate"
echo "them with a CloudFront distribution."
echo ""

# Maximum number of retries for operations
MAX_RETRIES=3

# Function to handle errors securely
handle_error() {
    local error_msg="$1"
    echo "ERROR: $error_msg" >&2
    echo "Check the log file for details: $LOG_FILE" >&2
    cleanup_resources
    exit 1
}

# Function to validate AWS CLI JSON output
validate_json() {
    local json_string="$1"
    if ! echo "$json_string" | jq empty 2>/dev/null; then
        return 1
    fi
    return 0
}

# Function to safely extract JSON values
extract_json_value() {
    local json_string="$1"
    local key_path="$2"

    if ! validate_json "$json_string"; then
```

```
        return 1
    fi

    echo "$json_string" | jq -r "$key_path" 2>/dev/null || return 1
}

# Function to clean up resources securely
cleanup_resources() {
    echo ""
    echo "=================================================="
    echo "CLEANING UP RESOURCES"
    echo "=================================================="

    if [ -n "${DISTRIBUTION_ID:-}" ] && [ -n "${WEB_ACL_ARN:-}" ]; then
        echo "Disassociating Web ACL from CloudFront distribution..."
        local account_id
        account_id=$(aws sts get-caller-identity --query Account --output text
 2>/dev/null) || account_id=""

        if [ -z "$account_id" ]; then
            echo "Warning: Could not retrieve AWS account ID"
            return
        fi

        local disassociate_result
        disassociate_result=$(aws wafv2 disassociate-web-acl \
            --resource-arn "arn:aws:cloudfront::${account_id}:distribution/
${DISTRIBUTION_ID}" \
            --region us-east-1 2>&1) || true

        if echo "$disassociate_result" | grep -qi "error"; then
            echo "Warning: Failed to disassociate Web ACL: $disassociate_result"
        else
            echo "Web ACL disassociated successfully."
        fi
    fi

    if [ -n "${WEB_ACL_ID:-}" ] && [ -n "${WEB_ACL_NAME:-}" ]; then
        echo "Deleting Web ACL..."

        local get_result
        get_result=$(aws wafv2 get-web-acl \
            --name "$WEB_ACL_NAME" \
            --scope CLOUDFRONT \
```

```
            --id "$WEB_ACL_ID" \
            --region us-east-1 2>&1) || true

        if echo "$get_result" | grep -qi "error"; then
            echo "Warning: Failed to get Web ACL for deletion: $get_result"
            echo "You may need to manually delete the Web ACL using the AWS
 Console."
        else
            local latest_token
            latest_token=$(extract_json_value "$get_result" '.WebACL.LockToken'
 2>/dev/null) || latest_token=""

            if [ -n "$latest_token" ]; then
                local delete_result
                delete_result=$(aws wafv2 delete-web-acl \
                    --name "$WEB_ACL_NAME" \
                    --scope CLOUDFRONT \
                    --id "$WEB_ACL_ID" \
                    --lock-token "$latest_token" \
                    --region us-east-1 2>&1) || true

                if echo "$delete_result" | grep -qi "error"; then
                    echo "Warning: Failed to delete Web ACL: $delete_result"
                    echo "You may need to manually delete the Web ACL using the
 AWS Console."
                else
                    echo "Web ACL deleted successfully."
                fi
            else
                echo "Warning: Could not extract lock token for deletion. You may
 need to manually delete the Web ACL."
            fi
        fi
    fi

    echo "Cleanup process completed."
}

# Security: Trap EXIT to ensure cleanup on any exit
trap cleanup_resources EXIT

# Generate a random identifier for resource names using secure method
RANDOM_ID=$(openssl rand -hex 4) || handle_error "Failed to generate random ID"
WEB_ACL_NAME="MyWebACL-${RANDOM_ID}"
```

```
METRIC_NAME="MyWebACLMetrics-${RANDOM_ID}"

echo "Using Web ACL name: $WEB_ACL_NAME"

# Step 1: Create a Web ACL
echo ""
echo "================================================="
echo "STEP 1: Creating Web ACL"
echo "================================================="

local create_result
create_result=$(aws wafv2 create-web-acl \
    --name "$WEB_ACL_NAME" \
    --scope "CLOUDFRONT" \
    --default-action Allow={} \
    --visibility-config
 "SampledRequestsEnabled=true,CloudWatchMetricsEnabled=true,MetricName=
$METRIC_NAME" \
    --tags Key=project,Value=doc-smith Key=tutorial,Value=aws-waf-gs \
    --region us-east-1 2>&1) || handle_error "Failed to create Web ACL"

if ! validate_json "$create_result"; then
    handle_error "Invalid JSON response from create-web-acl"
fi

# Extract Web ACL ID, ARN, and Lock Token from the response
WEB_ACL_ID=$(extract_json_value "$create_result" '.Summary.Id') || handle_error
 "Failed to extract Web ACL ID"
WEB_ACL_ARN=$(extract_json_value "$create_result" '.Summary.ARN') || handle_error
 "Failed to extract Web ACL ARN"
LOCK_TOKEN=$(extract_json_value "$create_result" '.Summary.LockToken') ||
 handle_error "Failed to extract Lock Token"

echo "Web ACL created successfully with ID: $WEB_ACL_ID"
echo "Lock Token: [REDACTED]"

# Step 2: Add a String Match Rule
echo ""
echo "================================================="
echo "STEP 2: Adding String Match Rule"
echo "================================================="

for ((i=1; i<=MAX_RETRIES; i++)); do
    echo "Attempt $i to add string match rule..."
```

```
    # Get the latest lock token before updating
    local get_result
    get_result=$(aws wafv2 get-web-acl \
        --name "$WEB_ACL_NAME" \
        --scope CLOUDFRONT \
        --id "$WEB_ACL_ID" \
        --region us-east-1 2>&1) || true

    if echo "$get_result" | grep -qi "error"; then
        echo "Warning: Failed to get Web ACL for update: $get_result"
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Failed to get Web ACL after $MAX_RETRIES attempts"
        fi
        sleep 2
        continue
    fi

    if ! validate_json "$get_result"; then
        echo "Warning: Invalid JSON response from get-web-acl"
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Invalid JSON response after $MAX_RETRIES attempts"
        fi
        sleep 2
        continue
    fi

    local latest_token
    latest_token=$(extract_json_value "$get_result" '.WebACL.LockToken' 2>/dev/
null) || true

    if [ -z "$latest_token" ]; then
        echo "Warning: Could not extract lock token for update"
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Failed to extract lock token after $MAX_RETRIES
 attempts"
        fi
        sleep 2
        continue
    fi

    local update_result
    update_result=$(aws wafv2 update-web-acl \
        --name "$WEB_ACL_NAME" \
```

```
        --scope "CLOUDFRONT" \
        --id "$WEB_ACL_ID" \
        --lock-token "$latest_token" \
        --default-action Allow={} \
        --rules '[{
            "Name": "UserAgentRule",
            "Priority": 0,
            "Statement": {
                "ByteMatchStatement": {
                    "SearchString": "MyAgent",
                    "FieldToMatch": {
                        "SingleHeader": {
                            "Name": "user-agent"
                        }
                    },
                    "TextTransformations": [
                        {
                            "Priority": 0,
                            "Type": "NONE"
                        }
                    ],
                    "PositionalConstraint": "EXACTLY"
                }
            },
            "Action": {
                "Count": {}
            },
            "VisibilityConfig": {
                "SampledRequestsEnabled": true,
                "CloudWatchMetricsEnabled": true,
                "MetricName": "UserAgentRuleMetric"
            }
        }]' \
        --visibility-config
 "SampledRequestsEnabled=true,CloudWatchMetricsEnabled=true,MetricName=
$METRIC_NAME" \
        --region us-east-1 2>&1) || true

    if echo "$update_result" | grep -qi "WAFOptimisticLockException"; then
        echo "Optimistic lock exception encountered. Will retry with new lock
 token."
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Failed to add string match rule after $MAX_RETRIES
 attempts"
```

```
        fi
        sleep 2
        continue
    elif echo "$update_result" | grep -qi "error"; then
        handle_error "Failed to add string match rule: $update_result"
    else
        echo "String match rule added successfully."
        break
    fi
done

# Step 3: Add AWS Managed Rules
echo ""
echo "=================================================="
echo "STEP 3: Adding AWS Managed Rules"
echo "=================================================="

for ((i=1; i<=MAX_RETRIES; i++)); do
    echo "Attempt $i to add AWS Managed Rules..."

    # Get the latest lock token before updating
    local get_result
    get_result=$(aws wafv2 get-web-acl \
        --name "$WEB_ACL_NAME" \
        --scope CLOUDFRONT \
        --id "$WEB_ACL_ID" \
        --region us-east-1 2>&1) || true

    if echo "$get_result" | grep -qi "error"; then
        echo "Warning: Failed to get Web ACL for update: $get_result"
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Failed to get Web ACL after $MAX_RETRIES attempts"
        fi
        sleep 2
        continue
    fi

    if ! validate_json "$get_result"; then
        echo "Warning: Invalid JSON response from get-web-acl"
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Invalid JSON response after $MAX_RETRIES attempts"
        fi
        sleep 2
        continue
```

```
    fi

    local latest_token
    latest_token=$(extract_json_value "$get_result" '.WebACL.LockToken' 2>/dev/
null) || true

    if [ -z "$latest_token" ]; then
        echo "Warning: Could not extract lock token for update"
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Failed to extract lock token after $MAX_RETRIES
 attempts"
        fi
        sleep 2
        continue
    fi

    local update_result
    update_result=$(aws wafv2 update-web-acl \
        --name "$WEB_ACL_NAME" \
        --scope "CLOUDFRONT" \
        --id "$WEB_ACL_ID" \
        --lock-token "$latest_token" \
        --default-action Allow={} \
        --rules '[{
            "Name": "UserAgentRule",
            "Priority": 0,
            "Statement": {
                "ByteMatchStatement": {
                    "SearchString": "MyAgent",
                    "FieldToMatch": {
                        "SingleHeader": {
                            "Name": "user-agent"
                        }
                    },
                    "TextTransformations": [
                        {
                            "Priority": 0,
                            "Type": "NONE"
                        }
                    ],
                    "PositionalConstraint": "EXACTLY"
                }
            },
            "Action": {
```

```
                "Count": {}
            },
            "VisibilityConfig": {
                "SampledRequestsEnabled": true,
                "CloudWatchMetricsEnabled": true,
                "MetricName": "UserAgentRuleMetric"
            }
        },
        {
            "Name": "AWS-AWSManagedRulesCommonRuleSet",
            "Priority": 1,
            "Statement": {
                "ManagedRuleGroupStatement": {
                    "VendorName": "AWS",
                    "Name": "AWSManagedRulesCommonRuleSet",
                    "ExcludedRules": []
                }
            },
            "OverrideAction": {
                "Count": {}
            },
            "VisibilityConfig": {
                "SampledRequestsEnabled": true,
                "CloudWatchMetricsEnabled": true,
                "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
            }
        }]' \
        --visibility-config
 "SampledRequestsEnabled=true,CloudWatchMetricsEnabled=true,MetricName=
$METRIC_NAME" \
        --region us-east-1 2>&1) || true

    if echo "$update_result" | grep -qi "WAFOptimisticLockException"; then
        echo "Optimistic lock exception encountered. Will retry with new lock
 token."
        if [ "$i" -eq "$MAX_RETRIES" ]; then
            handle_error "Failed to add AWS Managed Rules after $MAX_RETRIES
 attempts"
        fi
        sleep 2
        continue
    elif echo "$update_result" | grep -qi "error"; then
        handle_error "Failed to add AWS Managed Rules: $update_result"
    else
```

```
        echo "AWS Managed Rules added successfully."
        break
    fi
done

# Step 4: List CloudFront distributions
echo ""
echo "=================================================="
echo "STEP 4: Listing CloudFront Distributions"
echo "=================================================="

local cf_result
cf_result=$(aws cloudfront list-distributions --query "DistributionList.Items[*].
{Id:Id,DomainName:DomainName}" --output table 2>&1) || cf_result=""

if echo "$cf_result" | grep -qi "error"; then
    echo "Warning: Failed to list CloudFront distributions: $cf_result"
    echo "Continuing without CloudFront association."
    DISTRIBUTION_ID=""
else
    echo "$cf_result"

    # Auto-select first CloudFront distribution if available
    echo ""
    echo "=================================================="
    echo "STEP 5: Associate Web ACL with CloudFront Distribution"
    echo "=================================================="

    local first_dist
    first_dist=$(aws cloudfront list-distributions --query
 "DistributionList.Items[0].Id" --output text 2>&1) || first_dist=""

    if [ -n "$first_dist" ] && [ "$first_dist" != "None" ] && ! echo
 "$first_dist" | grep -qi "error"; then
        DISTRIBUTION_ID="$first_dist"
        echo "Using CloudFront distribution: $DISTRIBUTION_ID"

        local account_id
        account_id=$(aws sts get-caller-identity --query Account --output text
 2>/dev/null) || account_id=""

        if [ -z "$account_id" ]; then
            echo "Warning: Could not retrieve AWS account ID for association"
            DISTRIBUTION_ID=""
```

```
        else
            local associate_result
            associate_result=$(aws wafv2 associate-web-acl \
                --web-acl-arn "$WEB_ACL_ARN" \
                --resource-arn "arn:aws:cloudfront::${account_id}:distribution/
${DISTRIBUTION_ID}" \
                --region us-east-1 2>&1) || true

            if echo "$associate_result" | grep -qi "error"; then
                echo "Warning: Failed to associate Web ACL with CloudFront
 distribution: $associate_result"
                echo "Continuing without CloudFront association."
                DISTRIBUTION_ID=""
            else
                echo "Web ACL associated with CloudFront distribution
 successfully."
            fi
        fi
    else
        echo "No CloudFront distributions available. Skipping association."
        DISTRIBUTION_ID=""
    fi
fi

# Display summary of created resources
echo ""
echo "================================================="
echo "RESOURCE SUMMARY"
echo "================================================="
echo "Web ACL Name: $WEB_ACL_NAME"
echo "Web ACL ID: $WEB_ACL_ID"
echo "Web ACL ARN: $WEB_ACL_ARN"
if [ -n "${DISTRIBUTION_ID:-}" ]; then
    echo "Associated CloudFront Distribution: $DISTRIBUTION_ID"
fi
echo ""

# Auto-confirm cleanup
echo "================================================="
echo "CLEANUP CONFIRMATION"
echo "================================================="
echo "Proceeding with automatic cleanup of all created resources..."

echo ""
```

```
echo "================================================="
echo "Tutorial completed!"
echo "================================================="
echo "Log file: $LOG_FILE"
```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI.
  - AssociateWebAcl
  - CreateWebAcl
  - DeleteWebAcl
  - DisassociateWebAcl
  - GetCallerIdentity
  - GetWebAcl
  - ListDistributions
  - UpdateWebAcl

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Créez des URL signées et des cookies à l'aide d'un AWS Kit SDK

L'exemple de code suivant montre comment créer des URL et des cookies signés permettant d'accéder à des ressources restreintes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Utilisez la CannedSignerRequestclasse pour signer des URL ou des cookies avec une politique prédéfinie.

```
import software.amazon.awssdk.services.cloudfront.model.CannedSignerRequest;

import java.net.URL;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.time.Instant;
import java.time.temporal.ChronoUnit;

public class CreateCannedPolicyRequest {

    public static CannedSignerRequest createRequestForCannedPolicy(String
 distributionDomainName,
            String fileNameToUpload,
            String privateKeyFullPath, String publicKeyId) throws Exception {
        String protocol = "https";
        String resourcePath = "/" + fileNameToUpload;

        String cloudFrontUrl = new URL(protocol, distributionDomainName,
 resourcePath).toString();
        Instant expirationDate = Instant.now().plus(7, ChronoUnit.DAYS);
        Path path = Paths.get(privateKeyFullPath);

        return CannedSignerRequest.builder()
                .resourceUrl(cloudFrontUrl)
                .privateKey(path)
                .keyPairId(publicKeyId)
                .expirationDate(expirationDate)
                .build();
    }
}
```

Utilisez la CustomSignerRequestclasse pour signer des URL ou des cookies avec une politique personnalisée. Les `activeDate` et `ipRange` sont des méthodes facultatives.

```
import software.amazon.awssdk.services.cloudfront.model.CustomSignerRequest;

import java.net.URL;
import java.nio.file.Path;
import java.nio.file.Paths;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
```

```
public class CreateCustomPolicyRequest {

    public static CustomSignerRequest createRequestForCustomPolicy(String
 distributionDomainName,
            String fileNameToUpload,
            String privateKeyFullPath, String publicKeyId) throws Exception {
        String protocol = "https";
        String resourcePath = "/" + fileNameToUpload;

        String cloudFrontUrl = new URL(protocol, distributionDomainName,
 resourcePath).toString();
        Instant expireDate = Instant.now().plus(7, ChronoUnit.DAYS);
        // URL will be accessible tomorrow using the signed URL.
        Instant activeDate = Instant.now().plus(1, ChronoUnit.DAYS);
        Path path = Paths.get(privateKeyFullPath);

        return CustomSignerRequest.builder()
                .resourceUrl(cloudFrontUrl)
                // .resourceUrlPattern("https://*.example.com/*")  // Optional.
                .privateKey(path)
                .keyPairId(publicKeyId)
                .expirationDate(expireDate)
                .activeDate(activeDate) // Optional.
                // .ipRange("192.168.0.1/24") // Optional.
                .build();
    }
}
```

L'exemple suivant illustre l'utilisation de la CloudFrontUtilitiesclasse pour produire des cookies et des URL signés. Consultez cet exemple de code sur GitHub.

```
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import software.amazon.awssdk.services.cloudfront.CloudFrontUtilities;
import software.amazon.awssdk.services.cloudfront.cookie.CookiesForCannedPolicy;
import software.amazon.awssdk.services.cloudfront.cookie.CookiesForCustomPolicy;
import software.amazon.awssdk.services.cloudfront.model.CannedSignerRequest;
import software.amazon.awssdk.services.cloudfront.model.CustomSignerRequest;
import software.amazon.awssdk.services.cloudfront.url.SignedUrl;

public class SigningUtilities {
```

```
   private static final Logger logger =
LoggerFactory.getLogger(SigningUtilities.class);
   private static final CloudFrontUtilities cloudFrontUtilities =
CloudFrontUtilities.create();

   public static SignedUrl signUrlForCannedPolicy(CannedSignerRequest
cannedSignerRequest) {
       SignedUrl signedUrl =
cloudFrontUtilities.getSignedUrlWithCannedPolicy(cannedSignerRequest);
       logger.info("Signed URL: [{}]", signedUrl.url());
       return signedUrl;
   }

   public static SignedUrl signUrlForCustomPolicy(CustomSignerRequest
customSignerRequest) {
       SignedUrl signedUrl =
cloudFrontUtilities.getSignedUrlWithCustomPolicy(customSignerRequest);
       logger.info("Signed URL: [{}]", signedUrl.url());
       return signedUrl;
   }

   public static CookiesForCannedPolicy
getCookiesForCannedPolicy(CannedSignerRequest cannedSignerRequest) {
       CookiesForCannedPolicy cookiesForCannedPolicy = cloudFrontUtilities
               .getCookiesForCannedPolicy(cannedSignerRequest);
       logger.info("Cookie EXPIRES header [{}]",
cookiesForCannedPolicy.expiresHeaderValue());
       logger.info("Cookie KEYPAIR header [{}]",
cookiesForCannedPolicy.keyPairIdHeaderValue());
       logger.info("Cookie SIGNATURE header [{}]",
cookiesForCannedPolicy.signatureHeaderValue());
       return cookiesForCannedPolicy;
   }

   public static CookiesForCustomPolicy
getCookiesForCustomPolicy(CustomSignerRequest customSignerRequest) {
       CookiesForCustomPolicy cookiesForCustomPolicy = cloudFrontUtilities
               .getCookiesForCustomPolicy(customSignerRequest);
       logger.info("Cookie POLICY header [{}]",
cookiesForCustomPolicy.policyHeaderValue());
       logger.info("Cookie KEYPAIR header [{}]",
cookiesForCustomPolicy.keyPairIdHeaderValue());
       logger.info("Cookie SIGNATURE header [{}]",
cookiesForCustomPolicy.signatureHeaderValue());
```

```
        return cookiesForCustomPolicy;
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CloudFrontUtilitiesà la section Référence des AWS SDK for Java 2.x API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

CloudFront Exemples de fonctions pour CloudFront

Les exemples de code suivants montrent comment utiliser CloudFront les AWS SDK.

Exemples

- Ajouter des en-têtes de sécurité HTTP à un événement de réponse du visualiseur CloudFront Functions
- Ajouter un en-tête CORS à un événement de réponse de l'afficheur de CloudFront fonctions
- Ajouter un en-tête de contrôle du cache à un événement de réponse du visualiseur CloudFront Functions
- Ajouter un véritable en-tête IP client à un événement de demande du visualiseur CloudFront Functions
- Ajouter un en-tête d'origine à un événement de demande d'affichage de CloudFront fonctions
- Ajoutez index.html pour demander des URL sans nom de fichier dans un événement de demande de l'afficheur CloudFront Functions
- Normaliser les paramètres de chaîne de requête dans une demande d'affichage de CloudFront fonctions
- Redirection vers une nouvelle URL dans un événement de demande de l'afficheur CloudFront Functions
- Réécriture d'une URI de demande en fonction de la KeyValueStore configuration d'un événement de demande du visualiseur de CloudFront fonctions
- Acheminer les demandes vers une origine plus proche du visualiseur dans un événement de demande du visualiseur CloudFront Functions

- Utiliser des paires clé-valeur dans une demande d'affichage de CloudFront fonctions
- Valider un jeton simple dans une demande d'affichage de CloudFront fonctions

Ajouter des en-têtes de sécurité HTTP à un événement de réponse du visualiseur CloudFront Functions

L'exemple de code suivant montre comment ajouter des en-têtes de sécurité HTTP à un événement de réponse de l'afficheur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
async function handler(event) {
    var response = event.response;
    var headers = response.headers;

    // Set HTTP security headers
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation
    headers['strict-transport-security'] = { value: 'max-age=63072000;
 includeSubdomains; preload'};
    headers['content-security-policy'] = { value: "default-src 'none'; img-src
 'self'; script-src 'self'; style-src 'self'; object-src 'none'; frame-ancestors
 'none'"};
    headers['x-content-type-options'] = { value: 'nosniff'};
    headers['x-frame-options'] = {value: 'DENY'};
    headers['x-xss-protection'] = {value: '1; mode=block'};
    headers['referrer-policy'] = {value: 'same-origin'};

    // Return the response to viewers
    return response;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Ajouter un en-tête CORS à un événement de réponse de l'afficheur de CloudFront fonctions

L'exemple de code suivant montre comment ajouter un en-tête CORS à un événement de réponse de l'afficheur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
async function handler(event)  {
    var request = event.request;
    var response  = event.response;

    // If Access-Control-Allow-Origin CORS header is missing, add it.
    // Since JavaScript doesn't allow for hyphens in variable names, we use the
 dict["key"] notation.
    if (!response.headers['access-control-allow-origin'] &&
 request.headers['origin']) {
        response.headers['access-control-allow-origin'] = {value:
 request.headers['origin'].value};
        console.log("Access-Control-Allow-Origin was missing, adding it now.");
    }

    return response;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Ajouter un en-tête de contrôle du cache à un événement de réponse du visualiseur CloudFront Functions

L'exemple de code suivant montre comment ajouter un en-tête de contrôle du cache à un événement de réponse de l'afficheur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
async function handler(event) {
    var response = event.response;
    var headers = response.headers;

    if (response.statusCode >= 200 && response.statusCode < 400) {
        // Set the cache-control header
        headers['cache-control'] = {value: 'public, max-age=63072000'};
    }

    // Return response to viewers
    return response;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Ajouter un véritable en-tête IP client à un événement de demande du visualiseur CloudFront Functions

L'exemple de code suivant montre comment ajouter un véritable en-tête IP client à un événement de demande du visualiseur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
async function handler(event) {
    var request = event.request;
    var clientIP = event.viewer.ip;

    //Add the true-client-ip header to the incoming request
    request.headers['true-client-ip'] = {value: clientIP};

    return request;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Ajouter un en-tête d'origine à un événement de demande d'affichage de CloudFront fonctions

L'exemple de code suivant montre comment ajouter un en-tête d'origine à un événement de demande de l'afficheur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
async function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;

   // If origin header is missing, set it equal to the host header.
   if (!headers.origin)
       headers.origin = {value:`https://${host}`};

   return request;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Ajoutez index.html pour demander des URL sans nom de fichier dans un événement de demande de l'afficheur CloudFront Functions

L'exemple de code suivant montre comment ajouter index.html aux URL de demande sans nom de fichier dans un événement de demande de l'afficheur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
async function handler(event) {
    var request = event.request;
    var uri = request.uri;

    // Check whether the URI is missing a file name.
    if (uri.endsWith('/')) {
        request.uri += 'index.html';
    }
    // Check whether the URI is missing a file extension.
    else if (!uri.includes('.')) {
        request.uri += '/index.html';
    }

    return request;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Normaliser les paramètres de chaîne de requête dans une demande d'affichage de CloudFront fonctions

L'exemple de code suivant montre comment normaliser les paramètres de chaîne de requête dans une demande d'affichage de CloudFront fonctions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
function handler(event) {
     var qs=[];
     for (var key in event.request.querystring) {
         if (event.request.querystring[key].multiValue) {
             event.request.querystring[key].multiValue.forEach((mv) =>
 {qs.push(key + "=" + mv.value)});
         } else {
             qs.push(key + "=" + event.request.querystring[key].value);
         }
     };

     event.request.querystring = qs.sort().join('&');


     return event.request;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Redirection vers une nouvelle URL dans un événement de demande de l'afficheur CloudFront Functions

L'exemple de code suivant montre comment rediriger vers une nouvelle URL dans un événement de demande de l'afficheur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
async function handler(event) {
    var request = event.request;
    var headers = request.headers;
    var host = request.headers.host.value;
    var country = 'DE' // Choose a country code
    var newurl = `https://${host}/de/index.html`; // Change the redirect URL to
 your choice

    if (headers['cloudfront-viewer-country']) {
        var countryCode = headers['cloudfront-viewer-country'].value;
        if (countryCode === country) {
            var response = {
                statusCode: 302,
                statusDescription: 'Found',
                headers:
                    { "location": { "value": newurl } }
                }

            return response;
        }
    }
    return request;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Réécriture d'une URI de demande en fonction de la KeyValueStore configuration d'un événement de demande du visualiseur de CloudFront fonctions

L'exemple de code suivant montre comment réécrire un URI de demande en fonction de la KeyValueStore configuration d'un événement de demande de l'afficheur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
import cf from 'cloudfront';

// (Optional) Replace KVS_ID with actual KVS ID
const kvsId = "KVS_ID";
// enable stickiness by setting a cookie from origin or using another edge
 function
const stickinessCookieName = "appversion";
// set to true to enable console logging
const loggingEnabled = false;

// function rewrites the request uri based on configuration in KVS
// example config in KVS in key:value format
// "latest": {"a_weightage": .8, "a_url": "v1", "b_url": "v2"}
// given above key and value in KVS the request uri will be rewritten
// for example http(s)://domain/latest/something/else will be rewritten as
 http(s)://domain/v1/something/else or http(s)://domain/v2/something/else
 depending on weightage
// if no configuration is found, then the request is returned as is
async function handler(event) {
    // NOTE: This example function is for a viewer request event trigger.
    // Choose viewer request for event trigger when you associate this function
 with a distribution.
    const request = event.request;
    const pathSegments = request.uri.split('/');
```

```
    const key = pathSegments[1];

    // if empty path segment or if there is valid stickiness cookie
    // then skip call to KVS and let the request continue.
    if (!key || hasValidSticknessCookie(request.cookies[stickinessCookieName],
 key)) {
        return event.request;
    }

    try {
        // get the prefix replacement from KVS
        const replacement = await getPathPrefixByWeightage(key);
        if (!replacement) {
            return event.request;
        }
        //Replace the first path with the replacement
        pathSegments[1] = replacement;
        log(`using prefix ${pathSegments[1]}`)
        const newUri = pathSegments.join('/');
        log(`${request.uri} -> ${newUri}`);
        request.uri = newUri;

        return request;
    } catch (err) {
        // No change to the path if the key is not found or any other error
        log(`request uri: ${request.uri}, error: ${err}`);
    }
    // no change to path - return request
    return event.request;
}

// function to get the prefix from KVS
async function getPathPrefixByWeightage(key) {
    const kvsHandle = cf.kvs(kvsId);
    // get the weightage config from KVS
    const kvsResponse = await kvsHandle.get(key);
    const weightageConfig = JSON.parse(kvsResponse);
    // no configuration - return null
    if (!weightageConfig || !isFinite(weightageConfig.a_weightage)) {
        return null;
    }
    // return the url based on weightage
    // return null if no url is configured
    if (Math.random() <= weightageConfig.a_weightage) {
```

```
        return weightageConfig.a_url ? weightageConfig.a_url: null;
    } else {
        return weightageConfig.b_url ? weightageConfig.b_url : null;
    }
}

// function to check if the stickiness cookie is valid
function hasValidStickinessCookie(stickinessCookie, pathSegment) {
    // if the value exists and it matches pathSegment
    return (stickinessCookie && stickinessCookie.value === pathSegment)
}

function log(message) {
    if (loggingEnabled) {
        console.log(message);
    }
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Acheminer les demandes vers une origine plus proche du visualiseur dans un événement de demande du visualiseur CloudFront Functions

L'exemple de code suivant montre comment acheminer les demandes vers une origine plus proche du visualiseur dans le cadre d'un événement de demande du visualiseur CloudFront Functions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
import cf from 'cloudfront';
```

```
function handler(event) {
    const request = event.request;
    const headers = request.headers;
    const country = headers['cloudfront-viewer-country'] &&
        headers['cloudfront-viewer-country'].value;

    //List of Regions with S3 buckets containing content
    const countryToRegion = {
        'DE': 'eu-central-1',
        'IE': 'eu-west-1',
        'GB': 'eu-west-2',
        'FR': 'eu-west-3',
        'JP': 'ap-northeast-1',
        'IN': 'ap-south-1'
    };

    const DEFAULT_REGION = 'us-east-1';

    const selectedRegion = (country && countryToRegion[country]) ||
 DEFAULT_REGION;

    const domainName =
        `cloudfront-functions-demo-bucket-in-${selectedRegion}.s3.
${selectedRegion}.amazonaws.com`;

    cf.updateRequestOrigin({
        "domainName": domainName,
        "originAccessControlConfig": {
            "enabled": true,
            "region": selectedRegion,
            "signingBehavior": "always",
            "signingProtocol": "sigv4",
            "originType": "s3"
        },
    });

    return request;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser des paires clé-valeur dans une demande d'affichage de CloudFront fonctions

L'exemple de code suivant montre comment utiliser des paires clé-valeur dans une demande d'affichage de CloudFront fonctions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
import cf from 'cloudfront';

// This fails if there is no key value store associated with the function
const kvsHandle = cf.kvs();

// Remember to associate the KVS with your function before referencing KVS in
 your code.
// https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/kvs-with-
functions-associate.html
async function handler(event) {
    const request = event.request;
    // Use the first segment of the pathname as key
    // For example http(s)://domain/<key>/something/else
    const pathSegments = request.uri.split('/')
    const key = pathSegments[1]
    try {
        // Replace the first path of the pathname with the value of the key
        // For example http(s)://domain/<value>/something/else
        pathSegments[1] = await kvsHandle.get(key);
        const newUri = pathSegments.join('/');
        console.log(`${request.uri} -> ${newUri}`)
```

```
        request.uri = newUri;
    } catch (err) {
        // No change to the pathname if the key is not found
        console.log(`${request.uri} | ${err}`);
    }
    return request;
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Valider un jeton simple dans une demande d'affichage de CloudFront fonctions

L'exemple de code suivant montre comment valider un jeton simple dans une demande d' CloudFront affichage de fonctions.

JavaScript

JavaScript runtime 2.0 pour CloudFront Functions

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et apprenez à le configurer et à l'exécuter dans le référentiel d'exemples de CloudFront fonctions.

```
import crypto from 'crypto';
import cf from 'cloudfront';

//Response when JWT is not valid.
const response401 = {
    statusCode: 401,
    statusDescription: 'Unauthorized'
};

// Remember to associate the KVS with your function before calling the const
 kvsKey = 'jwt.secret'.
```

```
// https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/kvs-with-
functions-associate.html
const kvsKey = 'jwt.secret';
// set to true to enable console logging
const loggingEnabled = false;


function jwt_decode(token, key, noVerify, algorithm) {
    // check token
    if (!token) {
        throw new Error('No token supplied');
    }
    // check segments
    const segments = token.split('.');
    if (segments.length !== 3) {
        throw new Error('Not enough or too many segments');
    }

    // All segment should be base64
    const headerSeg = segments[0];
    const payloadSeg = segments[1];
    const signatureSeg = segments[2];

    // base64 decode and parse JSON
    const payload = JSON.parse(_base64urlDecode(payloadSeg));

    if (!noVerify) {
        const signingMethod = 'sha256';
        const signingType = 'hmac';

        // Verify signature. `sign` will return base64 string.
        const signingInput = [headerSeg, payloadSeg].join('.');

        if (!_verify(signingInput, key, signingMethod, signingType,
 signatureSeg)) {
            throw new Error('Signature verification failed');
        }

        // Support for nbf and exp claims.
        // According to the RFC, they should be in seconds.
        if (payload.nbf && Date.now() < payload.nbf*1000) {
            throw new Error('Token not yet active');
        }
```

```
        if (payload.exp && Date.now() > payload.exp*1000) {
            throw new Error('Token expired');
        }
    }

    return payload;
}

//Function to ensure a constant time comparison to prevent
//timing side channels.
function _constantTimeEquals(a, b) {
    if (a.length != b.length) {
        return false;
    }

    let xor = 0;
    for (let i = 0; i < a.length; i++) {
    xor |= (a.charCodeAt(i) ^ b.charCodeAt(i));
    }

    return 0 === xor;
}

function _verify(input, key, method, type, signature) {
    if(type === "hmac") {
        return _constantTimeEquals(signature, _sign(input, key, method));
    }
    else {
        throw new Error('Algorithm type not recognized');
    }
}

function _sign(input, key, method) {
    return crypto.createHmac(method, key).update(input).digest('base64url');
}

function _base64urlDecode(str) {
    return Buffer.from(str, 'base64url')
}

async function handler(event) {
    let request = event.request;

    //Secret key used to verify JWT token.
```

```
    //Update with your own key.
    const secret_key = await getSecret()

    if(!secret_key) {
        return response401;
    }

    // If no JWT token, then generate HTTP redirect 401 response.
    if(!request.querystring.jwt) {
        log("Error: No JWT in the querystring");
        return response401;
    }

    const jwtToken = request.querystring.jwt.value;

    try{
        jwt_decode(jwtToken, secret_key);
    }
    catch(e) {
        log(e);
        return response401;
    }

    //Remove the JWT from the query string if valid and return.
    delete request.querystring.jwt;
    log("Valid JWT token");
    return request;
}

// get secret from key value store
async function getSecret() {
    // initialize cloudfront kv store and get the key value
    try {
        const kvsHandle = cf.kvs();
        return await kvsHandle.get(kvsKey);
    } catch (err) {
        log(`Error reading value for key: ${kvsKey}, error: ${err}`);
        return null;
    }

}

function log(message) {
    if (loggingEnabled) {
```

```
        console.log(message);
    }
}
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation CloudFront avec un AWS Kit SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à CloudFront la documentation. Pour recevoir des notifications sur les mises à jour, vous pouvez vous abonner au flux RSS.

Modification	Description	Date
Ajout d'un TLS mutuel (afficheur)	CloudFront prend en charge le protocole TLS mutuel (afficheur).	24 novembre 2025
Ajout d'un champ de journal pour les journaux d'accès	Ajout du `connection-id` champ pour les journaux d'accès (journaux standard) et les journaux d'accès en temps réel.	24 novembre 2025
Journaux de connexion ajoutés	Ajout des journaux de connexion en tant que nouvelle fonctionnalité de journalisation pour le TLS mutuel (afficheur).	24 novembre 2025
Fonctions de connexion ajoutées	CloudFront prend en charge les fonctions de connexion pour le TLS mutuel (afficheur).	24 novembre 2025
Ajout de la prise en charge de l' CloudFront utilisation d'IPAM avec votre propre adresse IP	CloudFront permet de transférer vos propres adresses IPv4 via le BYOIP d'IPAM pour les services mondiaux.	24 novembre 2025
AWS mise à jour des politiques gérées	Les politiques `CloudFrontReadOnlyAccess` et `CloudFrontFullAccess` IAM soutiennent désormais `ec2:DescribeIpamPo`	24 novembre 2025

	`ols` et prennent des `ec2:GetIpamPoolCidrs` mesures.	
Mises à jour CloudFront des fonctions	Cette version ajoute des paramètres pour les méthodes d'assistance à la modification de l'origine dans CloudFront Functions . Vous pouvez utiliser les `originOverrides` paramètres `hostHeader` `sniallowedCertificate Names` ,, et.	20 novembre 2025
Mises à jour CloudFront des fonctions	Ajout de la prise en charge des jetons Web CBOR (CWT) pour les CloudFront fonctions.	20 novembre 2025
Mises à jour CloudFront des fonctions	Ajout de méthodes d'assista nce générales pour les CloudFront fonctions.	20 novembre 2025
Politique AWS gérée mise à jour	Mis `CloudFrontFullAcce ss` à jour pour autoriser la création d'une ressource ACL AWS WAF Web et l'accès à la création, à la mise à jour, à la suppression et à la lecture AWS du Pricing Plan Manager.	18 novembre 2025
Politique AWS gérée mise à jour	Mise `CloudFron tReadOnlyAccess` à jour pour accorder une autorisat ion en lecture seule au AWS Pricing Plan Manager.	18 novembre 2025

Politique AWS gérée mise à jour	Mis `CloudFrontFullAccess` à jour pour autoriser la création d'une ressource ACL AWS WAF Web et l'accès à la création, à la mise à jour, à la suppression et à la lecture AWS du Pricing Plan Manager.	18 novembre 2025
Politique AWS gérée mise à jour	Mise `CloudFrontReadOnlyAccess` à jour pour accorder une autorisation en lecture seule au AWS Pricing Plan Manager.	18 novembre 2025
CloudFront prend en charge les plans tarifaires forfaitaires	Vous pouvez désormais souscrire vos distributions à un plan tarifaire CloudFront forfaitaire.	18 novembre 2025
IP statiques en unidiffusion	Vous pouvez désormais choisir entre des adresses IPv4 uniquement ou à la fois des adresses IPv4 et IPv6 (dualstack).	5 novembre 2025

Ajout de la prise en charge du partage des origines des VPC entre Comptes AWS	Vous pouvez créer un partage de ressources et y ajouter des origines VPC. Cela vous permet de séparer les origines et les CloudFront distributions de votre VPC Comptes AWS, ce qui permet à votre organisation de respecter les exigences relatives à plusieurs comptes. D'autres Comptes AWS peuvent associer les origines VPC partagées à leurs CloudFront distributions.	5 novembre 2025
Ajout d’une politique de sécurité utilisateur	Ajout de la politique de sécurité TLSv1.2 _2025. • Protocoles et chiffrements pris en charge entre les spectateurs et CloudFront • Politique de sécurité (SSL/TLS version minimale)	10 octobre 2025
Ajout d’algorithmes d’échange de clés post-quantiques (PQ)	Ajout de deux nouveaux algorithmes d'échange de clés PQ aux politiques CloudFront TLS.	4 septembre 2025

Demandes d’origine en IPv6	Lorsque vous utilisez une origine personnalisée (à l'exception des origines Amazon S3 et VPC), vous pouvez personnaliser les paramètres d'origine de votre distribution afin de choisir comment CloudFront se connecte à votre origine à l'aide d'adresses IPv4 ou IPv6.	3 septembre 2025
Ajout d’une nouvelle politique de demande d’origine gérée	Ajout d’une nouvelle politique de demande d’origine gérée `HostHeaderOnly` .	29 août 2025
CloudFront les terminaux publics prennent désormais en charge IPv6	Consultez les CloudFront points de terminaison et les quotas Amazon dans le guide Références générales AWS de l'utilisateur Amazon VPC dans le guide de l'utilisateur Amazon VPC.Services AWS	21 août 2025
Ajout d’une politique de sécurité utilisateur	Ajout de TLSv1.3 _2025, une nouvelle politique de sécurité TLS 1.3 uniquement.	7 août 2025
Ajout de nouveaux paramètres de délai d’origine	Ajout du délai d’exécution de la réponse pour toutes les origines et du délai de réponse (délai de lecture de l’origine) pour les origines S3.	30 juillet 2025
Ajout de paramètres de distribution standard préconfigurés	Ajout de paramètres de distributions standard préconfigurés.	17 juin 2025

Ajout d'un nouveau flux de travail dans la console pour la configuration du domaine d'une distribution standard	Ajout d'un nouveau flux de travail dans la console pour la configuration du domaine d'une distribution standard.	17 juin 2025
Exemples de paramètres ajoutés	Ajout d'exemples montrant l'utilisation de paramètres avec des noms de domaine et des chemins d'origine dans les locataires de distribution.	17 juin 2025
Ajout de la prise en charge des CloudFront fonctions pour CloudFront SaaS Manager	Ajout de fonctions d'assistance et du champ `endpoint` pour l'objet `context`.	2 mai 2025
Mises à jour de la journalisation standard (v2)	Ajout de la variable de partition `{distributionid}` afin de prendre en charge l'envoi des journaux d'accès vers AWS Glue.	1er mai 2025
Mises à jour des politiques CloudFront gérées	Ajout des autorisations ACM aux politiques gérées `CloudFrontReadOnlyAccess` et `CloudFrontFullAccess` .	28 avril 2025

Ajout de la prise en charge des distributions multi-locataires et des locataires de distribution	Vous pouvez créer une distribution multi-locataires pour définir des paramètres de distribution communs en fonction du type d'origine. Vous pouvez ensuite réutiliser la distribution multi-locataires pour créer plusieurs locataires de distribution partageant ces paramètres. Vous pouvez ensuite personnaliser des locataires de distribution spécifiques à mesure que vous ajoutez des sites web ou des applications supplémentaires.	28 avril 2025
Mises à jour des fonctions Lambda@Edge	Les fonctions Lambda @Edge prennent désormais en charge les contrôles de journalisation avancés et la personnalisation du nom du groupe de CloudWatch journaux.	7 avril 2025
IP statiques en unidiffusion	Vous pouvez utiliser les adresses IP statiques Anycast pour activer le routage des domaines apex directement vers vos CloudFront distributions.	4 avril 2025
Ajout de méthodes d'assistance supplémentaires pour la modification de l'origine	Les méthodes d'assistance `selectRequestOriginById()` and `createRequestOriginGroup()` CloudFront Functions ont été ajoutées.	2 avril 2025

Mises à jour de la journalisation standard (v2)	Ajout de la variable de partition `{accountid}` et d'exemples de suffixes de chemin pour la livraison des journaux d'accès vers Amazon S3.	14 février 2025
Ajout de champs de journal d'accès en temps réel supplémentaires pour la journalisation standard (v2)	Vous pouvez spécifier les champs `c-country` et les champs du journal d'accès `cache-behavior-path-pattern` en temps réel lorsque vous activez la journalisation standard (v2).	31 janvier 2025
Lambda@Edge prend en charge la version d'environnement d'exécution la plus récente	Lambda @Edge prend désormais en charge les fonctions Lambda avec le runtime Node.js 22.	22 novembre 2024
Support de résilience tenant compte de la qualité des médias pour CloudFront	Vous pouvez utiliser la fonction MQAR (Media Quality Aware Resiliency) pour sélectionner CloudFront automatiquement l'origine dans un groupe d'origine présentant le score de qualité multimédia le plus élevé.	21 novembre 2024
Méthode d'assistance pour la modification de l'origine	Ajout d'une nouvelle méthode d'assistance CloudFront Functions pour la modification de l'origine.	21 novembre 2024

Origines VPC	Utilisez les origines CloudFront VPC pour restreindre l'accès à un équilibreur de charge d'application, à un équilibreur de charge réseau ou à une origine d'instance EC2.	20 novembre 2024
Mises à jour de la politique gérée	Politique gérée par `CloudFrontFullAccess` mise à jour.	20 novembre 2024
IP statiques en unidiffusion	Vous pouvez demander des adresses IP statiques Anycast CloudFront à utiliser avec vos distributions.	20 novembre 2024
Ajout de la prise en charge de la journalisation standard	CloudFront prend en charge la journalisation standard (v2) et l'envoi de vos CloudWatch journaux à Amazon Logs, Amazon Data Firehose et Amazon Simple Storage Service (Amazon S3).	20 novembre 2024
Ajout de la prise en charge de gRPC	CloudFront prend désormais en charge les requêtes gRPC pour votre distribution.	20 novembre 2024
Ajout d’une nouvelle politique gérée pour les origines VPC	Ajout de la nouvelle politique gérée `AWSCloudFrontVPCOriginServiceRolePolicy` .	20 novembre 2024
Lambda@Edge prend en charge la version d’environnement d’exécution la plus récente	Lambda@Edge prend désormais en charge les fonctions Lambda avec l’environnement d’exécution Python 3.13.	13 novembre 2024

Évaluez à l'aide de AWS Config règles	Évaluez vos CloudFront configurations à l'aide de AWS Config Rules.	20 septembre 2024
Ajout de contenu supplémentaire pour le dépannage	Ajout de contenu de dépannage supplémentaire pour les codes d'état de réponse HTTP 4xx et 5xx.	26 août 2024
Ajout de nouvelles politiques de cache gérées	Ajout des nouvelles politiques de cache gérées `UseOriginCacheControlHeaders` et `UseOriginCacheControlHeaders-QueryStrings` .	24 mai 2024
Ajout de la prise en charge du contrôle d'accès à d'origine	Vous pouvez désormais créer un contrôle d'accès à l'origine (OAC) pour la AWS Elemental MediaPackage V2 et l'URL de AWS Lambda la fonction.	11 avril 2024
Real-time champs du journal d'accès pour le CMCD	Ajout de 18 champs CMCD (Common Media Client Data) pour les journaux d'accès en temps réel.	9 avril 2024
Débuter avec une distribution CloudFront standard	Didacticiel mis à jour pour une distribution standard qui utilise une origine Amazon S3 avec un contrôle d'accès d'origine (OAC).	18 mars 2024

Exemples de code pour CloudFront l'utilisation des AWS kits de développement logiciel	Ajout d'exemples de code qui montrent comment utiliser CloudFront un kit de développement AWS logiciel (SDK). Les exemples sont divisés en extraits de code qui vous montrent comment appeler des fonctions de service individuelles et en exemples qui vous montrent comment accomplir une tâche spécifique en appelant plusieurs fonctions au sein d'un même service.	16 février 2024
AWS stratégie gérée	Les politiques IAM `CloudFrontReadOnlyAccess` et `CloudFrontFullAccess` prennent désormais en charge les opérations `KeyValueStore` .	19 décembre 2023
JavaScript exécution 2.0	Ajout de fonctionnalités JavaScript d'exécution 2.0 pour CloudFront Functions.	21 novembre 2023

CloudFront KeyValueStore	Amazon prend CloudFront désormais en charge CloudFront KeyValueStore. Cette fonctionnalité est une banque de données de valeurs de clé sécurisée, globale et à faible latence qui permet un accès en lecture depuis Functions. CloudFront Vous pouvez activer une logique personnalisable avancée aux emplacements CloudFront périphériques.	21 novembre 2023
Lambda@Edge prend en charge la version d'environnement d'exécution la plus récente	Lambda @Edge prend désormais en charge les fonctions Lambda avec le runtime Node.js 2.0.	15 novembre 2023
Tableau de bord de sécurité	CloudFront crée un tableau de bord de sécurité lorsque vous créez une distribution. Activez AWS WAF, gérez les restrictions géographiques et affichez des données de haut niveau pour les requêtes, les robots et les journaux.	8 novembre 2023
Tri des chaînes de requête dans les fonctions	CloudFront prend désormais en charge le tri des chaînes de requête à l'aide CloudFront de fonctions.	3 octobre 2023
AWS WAF recommandations de sécurité	Amazon affiche CloudFront désormais des recommandations AWS WAF de sécurité sur la CloudFront console.	26 septembre 2023

Prise en charge de la diffusion de contenu de cache obsolète (expiré)	CloudFront prend en charge `Stale-While-Revalidate` les directives de contrôle du `Stale-If-Error` cache et.	15 mai 2023
Activez AWS WAF les protections en un seul clic	Une méthode rationalisée pour ajouter des protections AWS WAF de sécurité aux CloudFront distributions.	10 mai 2023
Activer les listes ACL pour les nouveaux compartiments S3 utilisés pour les journaux standard	Ajout d'une note et de liens pour traiter le paramètre de liste ACL par défaut pour les nouveaux compartiments S3.	11 avril 2023
Création d'une origine à l'aide d'Amazon S3 Object Lambda	Vous pouvez utiliser un alias de point d'accès Amazon S3 Object Lambda comme origine pour votre distribution.	31 mars 2023
Personnalisez le statut et le corps du protocole HTTP à l'aide CloudFront des fonctions	Vous pouvez utiliser CloudFront Functions pour mettre à jour le code d'état de réponse du visualiseur et remplacer ou supprimer le corps de la réponse.	29 mars 2023
Ajout d'options de caractères génériques pour les en-têtes CORS pour les ports	Vous pouvez désormais inclure des configurations de caractères génériques pour les ports dans les en-têtes de contrôle d'accès CORS.	20 mars 2023

Ajout d'un nouveau lien pour le guide de AWS Security Hub CSPM l'utilisateur	Mise à jour de la langue et ajout d'un lien vers les CloudFront contrôles Amazon réorganisés dans le Guide de l'AWS Security Hub CSPM utilisateur.	9 mars 2023
CloudFront prend désormais en charge les listes de blocage (« tous sauf ») dans les politiques de demande d'origine	Utilisez des listes de blocage dans les politiques de demande d'origine pour inclure toutes les chaînes de requête, les en-têtes HTTP ou les cookies, à l'exception de ceux spécifiés, dans les requêtes CloudFront envoyées à l'origine.	22 février 2023
CloudFront ajoute une nouvelle politique de demande d'origine gérée pour transférer tous les en-têtes des spectateurs à l'exception de l'en-tête Host	Utilisez la CloudFront nouvelle politique de gestion des demandes d'origine pour inclure tous les en-têtes de la demande de l'utilisateur, à l'exception de l'`Host`en-tête, dans les demandes CloudFront envoyées à l'origine.	22 février 2023
Mise à jour des restrictions sur Lambda@Edge	Lambda@Edge prend en charge les configurations de gestion de l'environnement d'exécution Lambda définies sur Auto.	16 février 2023
Mise à jour des directives IAM pour CloudFront	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	15 février 2023

Renforcement de la sécurité avec contrôle d’accès à l’origine	Vous pouvez désormais sécuriser les MediaStore origines en n'autorisant l'accès qu'aux CloudFront distributions désignées.	9 février 2023
Nouveaux en-têtes pour déterminer la structure de l’en-tête d’un utilisateur	Vous pouvez désormais ajouter un ordre d’en-tête et un nombre d'en-têtes pour identifier l’utilisateur en fonction des en-têtes qu'il envoie.	13 janvier 2023
Lambda@Edge prend en charge la version d’environnement d’exécution la plus récente	Lambda @Edge prend désormais en charge les fonctions Lambda avec le runtime Node.js 18.	12 janvier 2023
Suppression des en-têtes de réponse à l'aide d'une politique d'en-têtes de réponse	Vous pouvez désormais utiliser une politique d'en-têtes de CloudFront réponse pour supprimer les en-têtes CloudFront reçus dans la réponse depuis l'origine. Les en-têtes spécifiés ne sont pas inclus dans la réponse envoyée CloudFront aux spectateurs.	3 janvier 2023
Déploiement continu pour tester en toute sécurité les changements de configuration	Vous pouvez désormais déployer les changements apportés à la configuration de votre CDN en effectuant des tests sur un sous-ensemble du trafic de production.	18 novembre 2022

Publication de l'en-tête `CloudFront-Viewer-JA3-Fingerprint`	Vous pouvez désormais utiliser l'empreinte JA3 pour déterminer si la demande provient d'un client connu.	16 novembre 2022
Ajout d'options génériques pour les en-têtes CORS	Vous pouvez désormais utiliser différentes configurations de caractères génériques dans certains en-têtes de contrôle d'accès CORS.	11 novembre 2022
Mesures supplémentaires pour les CloudFront distributions	Support pour `MonitoringSubscription` dans l' CloudFront API et CloudFormation.	3 octobre 2022
Renforcement de la sécurité avec contrôle d’accès à l’origine	Vous pouvez désormais sécuriser les origines d'Amazon S3 en autorisant l'accès uniquement aux CloudFront distributions désignées.	24 août 2022
HTTP/3 support pour les CloudFront distributions	Vous pouvez désormais choisir HTTP/3 votre CloudFront distribution.	15 août 2022
Ajouter les détails de la poignée de main à l'en-tête CloudFront-Viewer-TLS	Vous pouvez désormais consulter les informations relatives à la SSL/TLS poignée de main utilisée.	27 juin 2022
Nouvelle métrique dans l' Server-Timing en-tête	Ajout de la nouvelle métrique `cdn-downstream-fbl` aux en-têtes `Server-Timing` .	13 juin 2022

Nouvel en-tête pour obtenir des informations sur la version de TLS et le chiffrement TLS	Vous pouvez désormais utiliser l'`CloudFront-Viewer-TLS` en-tête pour obtenir des informations sur la version de TLS (ou SSL) et le chiffrement utilisé pour la connexion entre le visualiseur et. CloudFront	23 mai 2022
Nouvelle FunctionThrottles métrique pour les CloudFront fonctions	Avec Amazon CloudWatch, vous pouvez désormais contrôler le nombre de fois qu'une CloudFront fonction a été limitée au cours d'une période donnée.	4 mai 2022
CloudFront prend en charge les URL des fonctions Lambda	Si vous créez une application Web sans serveur à l'aide de fonctions Lambda avec des URL de fonction, vous pouvez désormais ajouter CloudFront de nombreux avantages.	6 avril 2022
Server-Timing en-tête dans les réponses HTTP	Vous pouvez désormais activer l'`Server-Timing` en-tête dans les réponses HTTP envoyées depuis CloudFront pour afficher les mesures qui peuvent vous aider à obtenir des informations sur le comportement et les performances de CloudFront.	30 mars 2022

Utiliser une liste de préfixes AWS gérée pour limiter le trafic entrant	Vous pouvez désormais limiter le trafic HTTP et HTTPS entrant vers vos origines uniquement à partir des adresses IP appartenant à des serveurs orientés vers l' CloudFront origine.	7 février 2022
Nouvelle fonction	CloudFront ajoute la prise en charge des politiques d'en-têtes de réponse, qui vous permettent de spécifier les en-têtes HTTP à CloudFron t ajouter aux réponses HTTP qu'il envoie aux spectateurs (navigateurs Web ou autres clients). Vous pouvez spécifier les en-têtes souhaités (et leurs valeurs) sans modifier l'origine ni écrire de code. Pour plus d'informations, consultez la section Ajouter ou supprimer des en-têtes HTTP dans les CloudFront réponses.	2 novembre 2021
Nouvel en-tête `CloudFron t-Viewer-Address` de demande	CloudFront ajoute la prise en charge d'un nouvel en-tête`CloudFront-Viewer-Address` ,, qui contient l'adresse IP de l'utilisateur à qui a envoyé la requête HTTP CloudFront. Pour plus d'informations, consultez la section Ajout d'en-têtes de CloudFront demande.	25 octobre 2021

Lambda@Edge prend en charge la nouvelle version d'environnement d'exécution	Lambda@Edge prend désormais en charge les fonctions Lambda avec l'environnement d'exécution Python 3.9. Pour plus d'informations, consultez Environnements d'exécution pris en charge.	22 septembre 2021
AWS mise à jour des politiques gérées	CloudFront a mis à jour la CloudFrontReadOnlyAccess politique. Pour plus d'informations, consultez la section CloudFront Mises à jour des politiques AWS gérées.	8 septembre 2021
Nouvelle fonction	CloudFront prend désormais en charge les certificats ECDSA pour les connexions HTTPS orientées vers le spectateur. Pour plus d'informations, consultez les sections Protocoles et chiffrements pris en charge entre les utilisateurs et CloudFront et Exigences relatives à l'utilisation de SSL/TLS certificats avec. CloudFront	14 juillet 2021

Nouvelle fonction	CloudFront prend désormais en charge davantage de moyens de déplacer un nom de domaine alternatif d'une distribution à une autre, sans contact Support. Pour plus d'informations, consultez Déplacement d'un nom de domaine alternatif vers une autre distribution.	7 juillet 2021
Nouvelle politique de sécurité	CloudFront prend désormais en charge une nouvelle politique de sécurité, TLSv1.2_2021, avec un ensemble plus restreint de chiffrements pris en charge. Pour plus d'informations, consultez la section Protocoles et chiffrements pris en charge entre les spectateurs et. CloudFront	23 juin 2021
Nouvelle fonction	Amazon prend CloudFront désormais en charge CloudFront Functions, une fonctionnalité native CloudFront qui vous permet d'écrire des fonctions légères JavaScript pour des personnalisations CDN à grande échelle et sensibles à la latence. Pour plus d'informations, consultez la section Personnalisation en périphérie à l'aide de CloudFront fonctions.	3 mai 2021

Lambda@Edge prend en charge les versions d'environnement d'exécution les plus récentes	Lambda @Edge prend désormais en charge les fonctions Lambda avec le runtime Node.js 14. Pour plus d'informations, consultez Environnements d'exécution pris en charge.	29 avril 2021
Supprimer la documentation des distributions RTMP	Amazon CloudFront a abandonné les distributions du protocole de messagerie en temps réel (RTMP) le 31 décembre 2020. La documentation relative aux distributions RTMP est désormais supprimée de l'Amazon CloudFront Developer Guide.	10 février 2021
Nouvelle option de tarification	Amazon CloudFront présente le forfait d'économies de CloudFront sécurité, un moyen simple d'économiser jusqu'à 30 % sur les CloudFront frais de votre AWS facture. Pour plus d'informations, consultez les FAQ sur les offres groupées Savings.	5 février 2021

Nouveau tutoriel	Le guide du CloudFront développeur Amazon inclut désormais un didacticiel sur l'utilisation d'Amazon pour restreindre l'accès CloudFront à un équilibreur de charge d'application dans Elastic Load Balancing. Pour plus d'informations, consultez Restriction de l'accès aux Application Load Balancers.	18 décembre 2020
Nouvelle option pour la gestion des clés publiques	CloudFront prend désormais en charge la gestion des clés publiques pour les URL signées et les cookies signés via la CloudFront console et l'API, sans avoir besoin d'accéder à l'utilisateur Compte AWS root. Pour plus d'informations, consultez Spécification des signataires qui peuvent créer des URL et des cookies signés.	22 octobre 2020

Nouvelle fonctionnalité : Origin Shield	CloudFront prend désormais en charge CloudFront Origin Shield, une couche supplémentaire de l'infrastructure de mise en CloudFront cache qui permet de minimiser la charge de votre origine, d'améliorer sa disponibilité et de réduire ses coûts d'exploitation. Pour plus d'informations, consultez la section Utilisation CloudFront d'Amazon Origin Shield.	20 octobre 2020
Nouveau format de compression	CloudFront prend désormais en charge la formation de compression Brotli lorsque vous configurez CloudFront pour compresser des objets aux emplacements CloudFront périphériques. Vous pouvez également configurer la mise CloudFront en cache des objets Brotli à l'aide d'un en-tête normaliséAccept-Encoding . Pour plus d'informations, consultez Service de fichiers compressés et Prise en charge de la compression.	14 septembre 2020

Nouveau protocole TLS	CloudFront prend désormais en charge le protocole TLS 1.3 pour les connexions HTTPS entre les spectateurs et les CloudFront distributions. Le protocole TLS 1.3 est activé par défaut dans toutes les politiques CloudFront de sécurité. Pour plus d'informations, consultez la section Protocoles et chiffrements pris en charge entre les spectateurs et. CloudFront	3 septembre 2020
Nouveaux journaux d'accès en temps réel	CloudFront prend désormais en charge les journaux d'accès en temps réel configurables. Grâce aux journaux d'accès en temps réel, vous pouvez obtenir des informations sur les demandes adressées à une distribution en temps réel. Vous pouvez utiliser les journaux d'accès en temps réel pour surveiller, analyser et prendre des mesures en fonction des performances de diffusion de contenu. Pour plus d'informations, consultez Real-time les journaux.	31 août 2020

Support de l'API pour des mesures supplémentaires	CloudFront prend désormais en charge l'activation de huit mesures supplémentaires en temps réel avec l' CloudFront API. Pour plus d'informations, consultez Activation de métriques supplémentaires.	28 août 2020
Nouveaux en-têtes CloudFront HTTP	CloudFront ajout d'en-têtes HTTP supplémentaires pour déterminer les informations relatives à l'utilisateur, telles que le type d'appareil, la localisation géographique, etc. Pour plus d'informations, consultez la section Ajout d'en-têtes de CloudFront demande.	23 juillet 2020
Nouvelle fonction	CloudFront prend désormais en charge les politiques de cache et les politiques de demande d'origine, ce qui vous donne un contrôle plus précis sur la clé de cache et les demandes d'origine pour vos CloudFront distributions. Pour plus d'informations, consultez les sections Contrôle de la clé de cache et Contrôle des demandes d'origine.	22 juillet 2020

Nouvelle politique de sécurité	CloudFront prend désormais en charge une nouvelle politique de sécurité, TLSv1.2_2019, avec un plus petit ensemble de chiffrements pris en charge. Pour plus d'informations, consultez la section Protocoles et chiffrements pris en charge entre les spectateurs et. CloudFront	8 juillet 2020
Nouveaux paramètres pour contrôler les délais et les tentatives d'origine	CloudFront a ajouté de nouveaux paramètres qui contrôlent les délais d'expiration et les tentatives d'origine. Pour plus d'informations, consultez Contrôle des délais d'expiration et des tentatives de l'origine.	5 juin 2020
Nouvelle documentation pour commencer à CloudFront créer un site Web statique sécurisé	Commencez CloudFront par créer un site Web statique sécurisé à l'aide d'Amazon S3 CloudFront, de Lambda @Edge, etc., tous déployés avec CloudFormation. Pour plus d'informations, consultez Démarrer avec un site web statique sécurisé.	2 juin 2020

Lambda@Edge prend en charge les versions d'environnement d'exécution les plus récentes	Lambda @Edge prend désormais en charge les fonctions Lambda avec les environnements d' Node.js exécution 12 et Python 3.8. Pour plus d'informations, consultez Environnements d'exécution pris en charge.	27 février 2020
Nouvelles mesures en temps réel dans CloudWatch	Amazon CloudFrontnow propose huit statistiques supplémentaires en temps réel sur Amazon CloudWatch. Pour plus d'informations, consultez la section Activation de mesures CloudFront de distribution supplémentaires.	19 décembre 2019
Nouveaux champs dans les journaux d'accès	CloudFront ajoute sept nouveaux champs aux journaux d'accès. Pour plus d'informations, consultez Champs d'un fichier journal standard.	12 décembre 2019
AWS WordPress plug-in	Vous pouvez utiliser le AWS WordPress plugin pour offrir aux visiteurs de votre WordPress site Web une expérience de visualisation accélérée en utilisant CloudFront. (Mise à jour : depuis le 30 septembre 2022, le WordPress plugin AWS for est obsolète.)	30 octobre 2019

Tag-based et politiques d'autorisations IAM au niveau des ressources	CloudFront prend désormais en charge deux méthodes supplémentaires pour spécifier les politiques d'autorisation IAM : les autorisations basées sur les balises et les autorisations au niveau des ressources. Pour plus d'informations, consultez Gestion de l'accès aux ressources.	8 août 2019
Support pour le langage de programmation Python	Vous pouvez désormais utiliser le langage de programmation Python pour développer des fonctions dans Lambda @Edge, en plus de Node.js. Pour obtenir des exemples de fonctions qui couvrent divers scénarios, consultez Exemples de fonctions Lambda@Edge.	1 août 2019
Graphiques de surveillance mis à jour	Le contenu est mis à jour pour décrire de nouvelles manières de surveiller les fonctions Lambda associées à vos CloudFront distributions directement depuis la CloudFront console afin de suivre et de déboguer plus facilement les erreurs. Pour de plus amples informations, veuillez consulter la section relative à la surveillance CloudFront.	20 juin 2019

Contenu de sécurité consolidé	Un nouveau chapitre consacré à la sécurité regroupe les informations relatives aux CloudFront fonctionnalités relatives à la protection des données, à l'IAM, à la journalisation, à la conformité et à leur mise en œuvre, et plus encore. Pour plus d'informations, consultez Sécurité.	24 mai 2019
La validation du domaine est désormais requise	CloudFront exige désormais que vous utilisiez un certificat SSL pour vérifier que vous êtes autorisé à utiliser un autre nom de domaine avec une distribution. Pour plus d'informations, consultez Utilisation de noms de domaines alternatifs et de HTTPS.	9 avril 2019
Nom de fichier PDF mis à jour	Le nouveau nom de fichier de l'Amazon CloudFront Developer Guide est : AmazonCloudFront_DevGuide. Le nom précédent était : cf-dg.	7 janvier 2019

Nouvelles fonctionnalités	CloudFront prend désormais WebSocket en charge un TCP-based protocole utile lorsque vous avez besoin de connexions de longue durée entre clients et serveurs. Vous pouvez également désormais configurer le basculement CloudFront d'origine pour les scénarios nécessitant une haute disponibilité. Pour plus d'informations, consultez Utilisation WebSocket avec les CloudFront distributions et Optimisation de la haute disponibilité avec CloudFront Origin Failover.	20 novembre 2018
Nouvelle fonction	CloudFront prend désormais en charge la journalisation détaillée des erreurs pour les requêtes HTTP qui exécutent des fonctions Lambda. Vous pouvez stocker les journaux CloudWatch et les utiliser pour résoudre les erreurs HTTP 5xx lorsque votre fonction renvoie une réponse non valide. Pour plus d'informations, consultez CloudWatch Métriques et CloudWatch journaux pour les fonctions Lambda.	8 octobre 2018

Nouvelle fonction	Vous pouvez désormais décider que Lambda@Edge expose le corps dans une requête pour des méthodes HTTP accessibles en écriture (POST, PUT, DELETE, etc.) afin que vous puissiez y accéder dans vos fonctions Lambda. Vous pouvez choisir un accès en lecture seule ou vous pouvez préciser que vous remplacerez le corps. Pour plus d'informations, consultez Accès au corps de la requête en choisissant l'option Inclure le corps.	14 août 2018
Nouvelle fonction	CloudFront prend désormais en charge la diffusion de contenu compressé à l'aide de brotli ou d'autres algorithmes de compression, en plus ou à la place de gzip. Pour plus d'informations, consultez Service de fichiers compressés.	25 juillet 2018
Réorganisation	L'Amazon CloudFront Developer Guide a été réorganisé afin de simplifier la recherche de contenus connexes et d'améliorer la scannabilité et la navigation.	28 juin 2018

Nouvelle fonctionnalité	Lambda@Edge vous permet désormais de personnaliser davantage la diffusion du contenu stocké dans un compartiment Amazon S3, en vous donnant accès à des en-têtes supplémentaires, y compris des en-têtes personnalisés, dans les événements orientés vers l'origine. Pour plus d'informations, consultez les exemples suivants illustrant la personnalisation de contenu selon l'emplacement de l'utilisateur et le type d'appareil de l'utilisateur.	20 mars 2018
Nouvelle fonctionnalité	Vous pouvez désormais utiliser Amazon CloudFront pour négocier des connexions HTTPS vers les origines à l'aide de l'algorithme de signature numérique Elliptic Curve (ECDSA). ECDSA utilise des clés plus petites donc plus rapides, mais tout aussi sécurisées que l'ancien algorithme RSA. Pour plus d'informations, consultez les sections SSL/TLS Protocoles et chiffrements pris en charge pour la communication entre CloudFront et votre origine et À propos des chiffrements RSA et ECDSA.	15 mars 2018

Nouvelle fonctionnalité	Lambda @Edge vous permet de personnaliser les réponses aux erreurs depuis votre origine, en vous permettant d'exécuter des fonctions Lambda en réponse à des erreurs HTTP CloudFront reçues provenant d'Amazon depuis votre origine. Pour plus d'informations, consultez les exemples suivants illustrant des redirections vers un autre emplacement et la génération d'une réponse avec un code de statut 200 (OK).	21 décembre 2017
Nouvelle fonctionnalité	Une nouvelle fonctionnalité CloudFront, le cryptage au niveau des champs, vous aide à renforcer la sécurité des données sensibles, telles que les numéros de carte de crédit ou les informations personnelles identifiables (PII) telles que les numéros de sécurité sociale. Pour plus d'informations, consultez Utilisation du chiffrement au niveau du champ pour protéger les données sensibles.	14 décembre 2017
Historique de la documentation archivé	Les anciens historiques du document a été archivé.	1er décembre 2017

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.