



Guide de l'utilisateur

Amazon EBS



Amazon EBS: Guide de l'utilisateur

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi 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 EBS ?	1
Fonctions d'Amazon EBS	1
Services connexes	2
Accès à Amazon EBS	3
Tarification	4
Configuration pour Amazon EBS	5
Inscrivez-vous pour Compte AWS	5
(Facultatif) Créez et utilisez une clé gérée par le client pour le chiffrement Amazon EBS	5
(Facultatif) Activer le blocage de l'accès public pour les instantanés Amazon EBS	6
Volumes EBS	8
Fonctionnalités et avantages	9
Disponibilité des données	9
Persistance des données	10
Chiffrement des données	11
Sécurité des données	11
Instantanés	12
Flexibilité	12
Types de volume EBS	13
Volumes de disque SSD (solid state drive)	13
Volumes de disque dur (HDD)	16
Volumes de la génération précédente	17
Volumes SSD à usage général	18
Volumes Provisioned IOPS SSD	23
Volumes HDD à débit optimisé et HDD à froid	27
Contraintes de volume EBS	38
Capacité de stockage	39
Limitations de service	39
Schémas de partitionnement	40
Tailles des blocs de données	41
Volumes EBS et NVMe	44
Associer les volumes aux noms des appareils	45
I/O délai de fonctionnement	49
Commande Abort	50
Cycle de vie des volumes	51

Créer un volume	53
Partager un volume	57
Copier un volume	63
Attacher un volume à une instance	70
Attacher un volume à plusieurs instances	73
Rendre un volume disponible à l'utilisation	82
Afficher des détails d'un volume	96
Modifier un volume	103
Détachez un volume d'une instance	129
Supprimer un volume	134
Remplacer un volume	135
Contrôles des statuts	139
Événements liés au volume	142
Utiliser un volume dégradé	144
Auto-enable I/O	148
Tests de défaillance	150
Expériences disponibles	150
Considérations	150
Suspendre l'injection par I/O défaut	151
Injection de latence	152
Instantanés EBS	157
Fonctionnement des instantanés	158
Cycle de vie du snapshot	162
Créer des instantanés	163
Afficher les informations d'instantané	170
Copie d'un instantané	174
Partager un instantané	189
Archiver des instantanés	196
Suppression d'un instantané	233
Restauration d'instantané rapide	238
Considérations	239
Tarification et facturation	239
Crédits de création de volume	240
Configurer la restauration rapide des instantanés	241
Vérifier l'état de restauration rapide des instantanés	244
Affichage des volumes restaurés à l'aide de la restauration d'instantané rapide	246

Verrouillage d'instantané	247
Concepts	248
Considérations	251
Contrôle d'accès	252
Verrouillage d'un instantané	256
Déverrouillage d'un instantané	259
Mise à jour des paramètres de verrouillage d'instantané	260
Verrouillage instantané du moniteur	261
Blocage de l'accès public pour les instantanés	264
Autorisations IAM	266
Configurer le blocage de l'accès public	267
Afficher le paramètre de blocage de l'accès public	271
Désactiver le blocage de l'accès public	274
Surveillez et bloquez l'accès public	277
Instantanés locaux sur Outposts	278
Questions fréquentes (FAQ)	279
Conditions préalables	282
Considérations	73
Contrôle de l'accès avec IAM	283
Utilisation des instantanés locaux	285
Instantanés locaux dans les zones locales	291
Questions fréquentes (FAQ)	279
Considérations	73
Contrôle de l'accès avec IAM	294
Chiffrement EBS	299
Fonctionnement du chiffrement EBS	299
Fonctionnement du chiffrement EBS lorsque le snapshot est chiffré	300
Fonctionnement du chiffrement EBS lorsque l'instantané est non chiffré	301
Comment les clés KMS inutilisables affectent les clés de données	301
Zones locales, avant-postes et zones de longueur d'onde	302
Local Zones	302
Avant-postes et zones de longueur d'onde	303
Exigences	303
Types de volume pris en charge	304
Types d'instance pris en charge	304
Autorisations pour les utilisateurs	304

Autorisations pour les instances	305
Activer le chiffrement par défaut	306
Clé de chiffrement par défaut	310
Chiffrer les ressources EBS	311
Chiffrer un volume vide lors de sa création	312
Chiffrer les ressources non chiffrées	312
Faire pivoter les clés KMS	313
Exemples	314
Restauration d'un volume non chiffré (chiffrement par défaut non activé)	315
Restauration d'un volume non chiffré (chiffrement par défaut activé)	315
Copie d'un instantané non chiffré (chiffrement par défaut non activé)	316
Copie d'un instantané non chiffré (chiffrement par défaut activé)	316
Re-encrypt un volume chiffré	317
Re-encrypt un instantané chiffré	317
Migration des données entre les volumes chiffrés et non chiffrés	318
Résultats du chiffrement	319
Performances EBS	322
Conseils sur les performances Amazon EBS	322
Utiliser des EBS-optimized instances	323
Configurer la bande passante de l'instance	323
Comprendre comment les performances sont calculées	323
Comprendre votre charge de travail	323
Être conscient des pertes de performances lors de l'initialisation des volumes à partir d'instantanés	323
Facteurs qui peuvent dégrader les performances des volumes HDD	324
Augmentez la lecture anticipée pour les charges de travail à haut débit et à lecture intensive sur st1 et sc1 (Instances Linux uniquement)	324
Utilisez un noyau Linux moderne (Instances Linux uniquement)	325
Utiliser RAID 0 pour optimiser l'utilisation des ressources d'instance	326
Surveillez les performances des volumes Amazon EBS	326
Optimisation EBS	327
Initialiser les volumes	327
Utiliser un tarif provisionné par Amazon EBS pour l'initialisation des volumes	328
Utiliser un instantané activé pour une restauration rapide	333
Initialiser manuellement les volumes	334
Initialisation du volume du moniteur	339

Pondération configurable de la bande passante des instances	343
I/O caractéristiques et surveillance	344
IOPS	345
Latence et longueur de file d'attente d'un volume	347
I/O limites de débit en termes de taille et de volume	348
Surveillez les I/O caractéristiques à l'aide CloudWatch	349
Surveillez les statistiques de I/O performance en temps réel	351
Ressources connexes	351
Configuration RAID	351
Options de configuration RAID	352
Création d'une matrice RAID 0	352
Créer des instantanés de volumes dans une grappe RAID	362
Comparer les volumes EBS	362
Configurer votre instance	363
Installer les outils d'évaluation	365
Choisir la longueur de la file d'attente d'un volume	366
Désactiver C-states	367
Effectuer la comparaison	368
Amazon Data Lifecycle Manager	373
Quotas	373
Comment ça marche	374
Stratégies	374
Planifications de politique	376
Target resource tags (Balises de ressource cibles)	377
Instantanés	377
EBS-backed AMI	377
Balises Amazon Data Lifecycle Manager	378
Politiques par défaut et politiques personnalisées	378
Comparaison des politiques d'instantanés EBS	379
EBS-backed Comparaison des politiques AMI	381
Création de politiques par défaut	383
Considérations relatives aux politiques par défaut	384
Création d'une politique par défaut pour les instantanés Amazon EBS	385
Création d'une politique par défaut pour les EBS-backed AMI	389
Activez les politiques par défaut pour tous les comptes et toutes les régions	393
Création d'une politique personnalisée pour les instantanés	398

Pour créer une stratégie de cycle de vie d'instantané	399
Considérations relatives aux stratégies de cycle de vie des instantanés	415
Ressources supplémentaires	421
Automatisez les instantanés cohérents avec les applications	422
Autres cas d'utilisation pour les pré-scripts et les post-scripts	459
Fonctionnement des pré-scripts et des post-scripts	468
Identifiez les instantanés créés à l'aide de scripts pré et post	471
Surveillez les pré-scripts et les post-scripts	472
Création d'une politique personnalisée pour les AMI	473
Pour créer une politique de cycle de vie d'AMI	473
Considérations relatives aux stratégies de cycle de vie des AMI	481
Ressources supplémentaires	484
Automatiser les copies d'instantanés entre comptes	485
Créer des politiques de copie d'instantané entre comptes	486
Spécifier les filtres de description d'instantané	498
Remarques relatives aux stratégies de copie d'instantané entre comptes	498
Ressources supplémentaires	499
Modifier les politiques	499
Suppression de politiques	502
Contrôle d'accès	504
AWS politiques gérées	506
Fonctions du service IAM	514
Surveiller les politiques	521
Console et AWS CLI	522
Surveillez les politiques à l'aide EventBridge	522
Surveillez les politiques à l'aide CloudWatch	524
Journalisation des appels d'API AWS CloudTrail avec	539
Points de terminaison de service	543
Points de terminaison IPv4	544
Dual-stack terminaux (IPv4 et IPv6)	544
Points de terminaison FIPS	544
Spécification des points de terminaison	545
Points de terminaison de VPC d'Interface	545
Considérations relatives aux points de terminaison Amazon EBS VPC	546
Création d'un point de terminaison VPC d'interface pour Amazon EBS	547
Dépannage	547

Erreur : le rôle dont le nom existe déjà	547
AWS Backup pour Amazon EBS	549
API directes Amazon EBS	550
Tarification	551
Tarification des API	551
Coûts de mise en réseau	551
Concepts	552
Instantanés	552
Blocs	552
Index de bloc	553
Jetons de bloc	553
Total de contrôle	553
Chiffrement	553
Actions d'API	553
Signature Version 4 (signature)	554
Contrôle d'accès	555
Lire les instantanés	560
Liste des blocs dans un instantané	561
Liste des blocs qui sont différents entre deux instantanés	564
Obtenir des données de bloc à partir d'un instantané	567
Écrire des instantanés	569
Démarrer un instantané	570
Ajouter des données dans un instantané	572
Terminer un instantané	574
Résultats du chiffrement	575
Résultats du chiffrement : instantané parent non chiffré	576
Résultats du chiffrement : instantané parent chiffré	576
Résultats du chiffrement : aucun instantané parent	577
Valider les données de capture	578
Garantir l'idempotence	579
Tentatives d'erreurs	580
Optimiser les performances	584
Points de terminaison de service	585
Points de terminaison IPv4	585
Dual-stack points de terminaison (IPv4 et IPv6)	586
Points de terminaison FIPS	587

Spécification des points de terminaison	587
Exemples de code SDK	589
StartSnapshot	589
PutSnapshotBlock	590
CompleteSnapshot	591
Points de terminaison de VPC d'Interface	592
Considérations relatives aux points de terminaison VPC des API directes EBS	592
Créer un point de terminaison d'un VPC d'interface pour les API directes EBS	593
CloudTrail journaux	594
EBS dirige les événements de données des API dans CloudTrail	596
Événements de gestion directe des API EBS dans CloudTrail	597
Exemples d'événements liés aux API EBS Direct	540
FAQ	603
Corbeille	606
Ressources prises en charge	607
Fonctionnement	608
Considérations	609
Quotas	613
Services connexes	613
Tarification	613
Contrôle d'accès	614
Autorisations pour utiliser la corbeille et les règles de rétention	615
Autorisations pour utiliser des ressources dans la corbeille	616
Clés de condition pour la corbeille	617
Créer une règle de rétention	620
Mettre à jour la règle de conservation	624
Règle de rétention des verrous	626
Déverrouiller la règle de rétention	628
Étiqueter des règles de rétention	630
Afficher les identifications de règle de rétention	631
Supprimer les identifications des règles de rétention	632
Supprimer les règles de conservation	633
Récupérer des instantanés supprimés	634
Autorisations pour utiliser des instantanés dans la corbeille	634
Afficher les instantanés dans la corbeille	635
Restaurer des instantanés à partir de la corbeille	637

Restaurer les volumes supprimés	638
Autorisations pour travailler avec des volumes dans la corbeille	638
Afficher les volumes dans la corbeille	640
Restaurer les volumes depuis la corbeille	642
Récupérer les AMI supprimées	643
Autorisations pour utiliser des AMI dans la corbeille	643
Afficher les AMI dans la corbeille	644
Restaurer des AMI depuis la corbeille	646
Moniteur utilisant EventBridge	647
RuleLocked	648
RuleChangeAttempted	648
RuleUnlockScheduled	649
RuleUnlockingNotice	650
RuleUnlocked	650
Moniteur utilisant CloudTrail	651
Informations sur la corbeille dans CloudTrail	539
Comprendre les entrées du fichier journal de la corbeille	653
Points de terminaison de service	666
Points de terminaison IPv4	585
Dual-stack terminaux (IPv4 et IPv6)	667
Points de terminaison FIPS	668
Spécification des points de terminaison	668
Utiliser les points de terminaison VPC de l'interface	669
Créer un point de terminaison VPC d'interface pour la corbeille	669
Création d'une politique de point de terminaison VPC pour la corbeille	669
Sécurité	671
Protection des données	671
Sécurité des données Amazon EBS	673
Chiffrement au repos et en transit	673
Gestion des clés KMS	673
Gestion des identités et des accès	674
Public ciblé	675
Authentification par des identités	675
Gestion de l'accès à l'aide de politiques	677
Comment EBS fonctionne avec IAM	678
Exemple de politiques IAM	684

Dépannage	704
Validation de conformité	706
Résilience des données	706
Contrôle	708
Amazon CloudWatch	709
Métriques pour les volumes Amazon EBS	709
Statistiques pour les instantanés Amazon EBS	737
Métriques d'instances Nitro	737
Métriques de restauration d'instantané rapide	742
Graphiques de la console Amazon EC2	744
Amazon EventBridge	746
Événements de volume EBS	747
Événement d'initialisation du volume EBS	753
Événements de modification de volume EBS	754
Événements d'instantané EBS	754
Événements d'archivage d'instantanés EBS	763
Événements de restauration d'instantané rapide EBS	763
Utilisation AWS Lambda pour gérer les EventBridge événements	764
Statistiques de performance détaillées d'EBS	768
Statistiques	768
Accès aux statistiques	771
Amazon GuardDuty	773
Rapports d'utilisation et de facturation	774
Instantanés	774
Stockage de volume	775
Performances provisionnées	776
API directes EBS	777
Restauration rapide des instantanés (FSR)	778
Dressez l'inventaire de vos volumes EBS	778
Volumes	779
I/O performance	781
Contenu de vos volumes de données EBS	782
Instantanés	783
Contenu de vos instantanés EBS	783
Quotas	785
Historique de la documentation	805

..... dcccix

Qu'est-ce qu'Amazon Elastic Block Store ?

Amazon Elastic Block Store (Amazon EBS) fournit des ressources de stockage par blocs évolutives et hautes performances qui peuvent être utilisées avec les instances Amazon Elastic Compute Cloud (Amazon EC2). Avec Amazon Elastic Block Store, vous pouvez créer et gérer les ressources de stockage par blocs suivantes :

- **Volumes Amazon EBS** : il s'agit de volumes de stockage que vous attachez aux instances Amazon EC2. Après avoir associé un volume à une instance, vous pouvez l'utiliser de la même manière que vous utiliseriez un disque dur local connecté à un ordinateur, par exemple pour stocker des fichiers ou installer des applications.
- **Instantanés Amazon EBS** : il s'agit de sauvegardes ponctuelles de volumes Amazon EBS qui sont conservées indépendamment du volume lui-même. Vous pouvez créer des instantanés pour sauvegarder les données sur vos volumes Amazon EBS. Vous pouvez ensuite restaurer de nouveaux volumes à partir de ces instantanés à tout moment.

Rubriques

- [Fonctions d'Amazon EBS](#)
- [Services connexes](#)
- [Accès à Amazon EBS](#)
- [Tarification](#)

Fonctions d'Amazon EBS

Amazon EBS propose les fonctionnalités et avantages suivants :

- **Plusieurs types de volumes** : Amazon EBS propose plusieurs types de volumes qui vous permettent d'optimiser les performances et les coûts de stockage pour un large éventail d'applications. Les types de volumes sont divisés en deux grandes catégories : le **SSD-backed stockage** pour les charges de travail transactionnelles et le **HDD-backed stockage** pour les charges de travail gourmandes en débit.
- **Évolutivité** : vous pouvez créer des volumes Amazon EBS avec des spécifications de capacité et de performances qui répondent à vos besoins. Au fur et à mesure de l'évolution de vos besoins, vous pouvez utiliser les opérations Elastic Volumes pour augmenter dynamiquement la capacité ou optimiser les performances, sans interruption de service.

- **Sauvegarde et restauration** : utilisez les instantanés Amazon EBS pour sauvegarder les données stockées sur vos volumes. Vous pouvez ensuite utiliser ces instantanés pour restaurer instantanément des volumes ou pour migrer des données entre des AWS comptes, des AWS régions ou des zones de disponibilité.
- **Protection des données** : utilisez le chiffrement Amazon EBS pour chiffrer vos volumes Amazon EBS et vos instantanés Amazon EBS. Les opérations de chiffrement ont lieu sur les serveurs qui hébergent les instances Amazon EC2. Cela garantit la sécurité des données au repos et des données en transit entre une instance et son volume attaché, ainsi que les instantanés suivants.
- **Disponibilité et durabilité des données** : les volumes io2 Block Express offrent une durabilité de 99,999 % avec un taux de défaillance annuel de 0,001 %. Les autres types de volume offrent une durabilité de 99,8 % à 99,9 % avec un taux de défaillance annuel de 0,1 % à 0,2 %. En outre, les volumes de données sont automatiquement répliqués sur plusieurs serveurs d'une zone de disponibilité afin d'éviter toute perte de données due à la défaillance d'un composant.
- **Archivage des données** : EBS Snapshots Archive fournit un niveau de stockage économique permettant d'archiver des copies complètes et instantanées d'EBS Snapshots. Utilisez Archive lorsque vous devez conserver des instantanés pendant 90 jours ou plus à des fins réglementaires, de conformité ou de publication future de projets.

Services connexes

Amazon EBS fonctionne avec les services suivants :

- **Amazon Elastic Compute Cloud** : service qui vous permet de lancer et de gérer des machines virtuelles (instances Amazon EC2) dans le AWS cloud. Vous pouvez associer des volumes EBS à ces instances et les utiliser de la même manière que vous utiliseriez un disque dur local, par exemple pour stocker des fichiers ou installer des applications. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon EC2 ?](#)
- **AWS Key Management Service**— Service géré qui vous permet de créer et de gérer des clés cryptographiques. Vous pouvez utiliser des clés AWS KMS cryptographiques pour chiffrer les données stockées sur vos volumes Amazon EBS et dans vos instantanés Amazon EBS. Pour plus d'informations, consultez [Comment Amazon EBS utilise AWS KMS](#).
- **Amazon Data Lifecycle Manager** : service géré qui automatise la création, la conservation et la suppression des instantanés EBS et des AMI. EBS-backed Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser les sauvegardes de vos volumes Amazon EBS et de vos

instances Amazon EC2. Pour de plus amples informations, veuillez consulter [Automatisez les sauvegardes avec Amazon Data Lifecycle Manager](#).

- **API EBS direct** : service qui vous permet de créer des instantanés EBS, d'écrire des données directement dans vos instantanés, de lire les données de vos instantanés et d'identifier les différences ou les modifications entre deux instantanés. Pour de plus amples informations, veuillez consulter [Utiliser API directes EBS pour accéder au contenu d'un instantané EBS](#).
- **Corbeille** : service de récupération de données qui vous permet de restaurer des instantanés et EBS-backed AMI EBS supprimés accidentellement. Pour plus d'informations, voir [Corbeille](#).

Accès à Amazon EBS

Vous pouvez créer et gérer vos ressources Amazon EBS à l'aide des interfaces suivantes :

Console Amazon EC2

Interface Web permettant de créer et de gérer des volumes et des instantanés. Si vous avez créé un AWS compte, vous pouvez accéder à la console Amazon EC2 à <https://console.aws.amazon.com/ec2/> l'adresse.

AWS Command Line Interface

Outil de ligne de commande qui vous permet de gérer les ressources Amazon EBS à l'aide des commandes de votre interface de ligne de commande. Elle est prise en charge sur Windows, Mac et Linux. Pour plus d'informations, consultez le Guide de [AWS Command Line Interface l'utilisateur](#) et les commandes <https://docs.aws.amazon.com/cli/latest/reference/ec2/> ec2.

Outils AWS pour PowerShell

Ensemble de PowerShell modules qui vous permettent d'exécuter des opérations par script sur vos ressources Amazon EBS à partir de la ligne de PowerShell commande. Pour plus d'informations, consultez le Guide de l'[Outils AWS pour PowerShell utilisateur](#) et la référence des [Outils AWS pour PowerShell applets de commande](#).

CloudFormation

AWS Service entièrement géré qui vous permet de créer des modèles JSON ou YAML réutilisables qui décrivent vos AWS ressources, puis de provisionner et de configurer ces ressources pour vous. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS CloudFormation](#).

API de requête Amazon EC2

L'API Amazon EC2 Query fournit des requêtes HTTP ou HTTPS qui utilisent le verbe HTTP GET ou POST et un paramètre de requête nommé `Action`. Pour plus d'informations, consultez la référence [de l'API](#) Amazon EC2.

AWS SDK

Language-specific Des API qui vous permettent de créer des applications intégrées à des AWS services. AWS Des kits SDK sont disponibles pour de nombreux langages de programmation courants. Pour plus d'informations, consultez la section [Outils sur lesquels s'appuyer AWS](#).

Tarification

Avec Amazon EBS, vous ne payez que ce que vous allouez. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Configuration pour Amazon EBS

Effectuez les tâches décrites dans cette section pour vous préparer à utiliser les ressources Amazon EBS.

Tâches

- [Inscrivez-vous pour Compte AWS](#)
- [\(Facultatif\) Créez et utilisez une clé gérée par le client pour le chiffrement Amazon EBS](#)
- [\(Facultatif\) Activer le blocage de l'accès public pour les instantanés Amazon EBS](#)

Inscrivez-vous pour Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Pour plus d'informations sur la création d'un Compte AWS, consultez la section [Démarrage avec un Compte AWS](#) dans le Guide de Gestion de compte AWS référence.

(Facultatif) Créez et utilisez une clé gérée par le client pour le chiffrement Amazon EBS

Le chiffrement Amazon EBS est une solution de chiffrement qui utilise des clés AWS KMS cryptographiques pour chiffrer vos volumes Amazon EBS et vos instantanés Amazon EBS. Amazon EBS crée automatiquement une clé KMS AWS gérée unique pour le chiffrement Amazon EBS dans chaque région. Cette clé KMS possède l'alias `aws/ebs`. Vous ne pouvez pas modifier la clé KMS par défaut ni gérer ses autorisations. Pour plus de flexibilité et de contrôle sur la clé KMS utilisée pour le chiffrement Amazon EBS, vous pouvez envisager de créer et d'utiliser une clé gérée par le client.

Pour créer et utiliser une clé gérée par le client pour le chiffrement Amazon EBS

1. [Créez une clé](#) KMS de chiffrement symétrique.
2. [Sélectionnez la clé KMS comme clé KMS par défaut pour le chiffrement Amazon EBS.](#)
3. [Autorisez les utilisateurs à utiliser la clé KMS pour le chiffrement](#) Amazon EBS.

(Facultatif) Activer le blocage de l'accès public pour les instantanés Amazon EBS

Pour empêcher le partage public de vos instantanés, vous pouvez activer le blocage de l'accès public pour les instantanés. Une fois que vous avez activé le blocage de l'accès public pour les instantanés dans une région, toute tentative de partage public d'instantanés dans cette région est automatiquement bloquée. Cela peut vous aider à améliorer la sécurité de vos instantanés et à protéger les données de vos instantanés contre tout accès non autorisé ou involontaire.

Pour plus d'informations, consultez [Bloquer l'accès public aux instantanés Amazon EBS](#).

Console

Pour activer le blocage de l'accès public pour les instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Tableau de bord EC2, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. Dans la section Bloquer l'accès public pour les instantanés EBS, choisissez Gérer.
4. Sélectionnez Bloquer l'accès public, puis choisissez l'une des options suivantes :
 - Bloquer tous les accès publics : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
 - Bloquer les nouveaux partages publics : pour bloquer tout nouveau partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.
5. Choisissez Mettre à jour.

AWS CLI

Pour activer le blocage de l'accès public pour les instantanés

Utilisez la commande [enable-snapshot-block-public-access](#). Pour `--state`, spécifiez l'une des valeurs suivantes :

- `block-all-sharing` : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- `block-new-sharing` : pour bloquer uniquement les nouveaux partages publics de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

```
aws ec2 enable-snapshot-block-public-access --state block-new-sharing
```

PowerShell

Pour activer le blocage de l'accès public pour les instantanés

Utilisez l'applet de commande [Enable-EC2SnapshotBlockPublicAccess](#). Pour `-State`, spécifiez l'une des valeurs suivantes :

- `block-all-sharing` : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- `block-new-sharing` : pour bloquer uniquement les nouveaux partages publics de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

```
Enable-EC2SnapshotBlockPublicAccess -State block-new-sharing
```

Volumes Amazon EBS

Un volume Amazon EBS est un dispositif de stockage durable au niveau bloc que vous pouvez attacher à vos instances. Après avoir attaché un volume à une instance, vous pouvez l'utiliser comme n'importe quel autre disque dur physique. Les volumes EBS sont flexibles. Pour des volumes de génération actuelle attachés à des types d'instances de génération actuelle, vous pouvez augmenter dynamiquement la taille, modifier la capacité IOPS provisionnée et changer le type des volumes de production en direct.

Vous pouvez utiliser des volumes EBS comme stockage principal pour des données nécessitant des mises à jour fréquentes, telles que le lecteur système pour une instance ou le stockage pour une application de base de données. Vous pouvez également les utiliser pour les applications à débit élevé qui effectuent des analyses continues du disque. Les volumes EBS sont permanents indépendamment de la durée d'exécution d'une instance EC2.

Vous pouvez également attacher plusieurs volumes EBS à une seule instance. Le volume et l'instance doivent être dans la même zone de disponibilité. Selon les types de volume et d'instance, vous pouvez [Multi-Attach](#) monter un volume sur plusieurs instances en même temps.

Amazon EBS fournit les types de volumes suivants : SSD à usage général (gp2 et gp3), SSD IOPS provisionnés (io1 et io2), HDD optimisé pour le débit (st1), HDD à froid (sc1) et magnétique (standard). Ils se distinguent par leurs caractéristiques de performance et leurs tarifs, ce qui vous permet d'adapter vos performances de stockage et vos coûts en fonction des besoins de vos applications. Pour plus d'informations, consultez [Types de volume Amazon EBS](#).

Votre compte a une limite sur le stockage total dont vous disposez. Pour plus d'informations sur ces limites et pour savoir comment demander leur augmentation, consultez [Points de terminaison et quotas Amazon EBS](#) (français non garanti).

Un volume EBS géré est géré par un fournisseur de services, tel qu'Amazon EKS Auto Mode. Vous ne pouvez pas modifier directement les paramètres d'un volume EBS géré. Les volumes EBS gérés sont identifiés par une valeur vraie dans le champ Géré. Pour plus d'informations, consultez la section Instances [gérées](#) Amazon EC2.

Pour plus d'informations sur la tarification, consultez [Tarification Amazon EBS](#).

Table des matières

- [Caractéristiques et avantages des volumes Amazon EBS](#)

- [Types de volume Amazon EBS](#)
- [Contraintes de volume Amazon EBS](#)
- [Volumes Amazon EBS et NVMe](#)
- [Cycle de vie des volumes Amazon EBS](#)
- [Remplacer un volume Amazon EBS à l'aide d'un instantané](#)
- [Vérifications de l'état des volumes Amazon EBS](#)
- [Tests de défaillance sur Amazon EBS](#)

Caractéristiques et avantages des volumes Amazon EBS

Les volumes EBS offrent des avantages supplémentaires par rapport aux volumes de stockage d'instances.

Avantages

- [Disponibilité des données](#)
- [Persistance des données](#)
- [Chiffrement des données](#)
- [Sécurité des données](#)
- [Instantanés](#)
- [Flexibilité](#)

Disponibilité des données

Lorsque vous créez un volume EBS, il est automatiquement répliqué au sein la zone de disponibilité pour empêcher toute perte de données consécutive à la défaillance d'un composant matériel. Vous pouvez attacher un volume EBS à n'importe quelle instance EC2 dans la même zone de disponibilité. Une fois qu'un volume est attaché, il se présente comme un périphérique de stockage en mode bloc natif similaire à un disque dur ou à un autre périphérique physique. À ce stade, l'instance peut interagir avec le volume de la même façon qu'avec un périphérique local. Vous pouvez vous connecter à l'instance et formater le volume EBS avec un système de fichiers, par exemple Ext4 pour une instance Linux ou NTFS pour une instance Windows, puis installer des applications.

Si vous associez plusieurs volumes à un appareil que vous avez nommé, vous pouvez répartir les données entre les volumes pour améliorer I/O les performances en termes de débit.

Vous pouvez associer `io1` des volumes `io2` EBS à 16 Nitro-based instances au maximum. Pour plus d'informations, consultez [Attachez un volume EBS à plusieurs instances EC2 à l'aide de Multi-Attach](#). Sinon, vous pouvez attacher un volume EBS à une seule instance.

Vous pouvez obtenir des données de surveillance pour vos volumes EBS, y compris les volumes du périphérique racine pour les EBS-backed instances, sans frais supplémentaires. Pour plus d'informations sur la surveillance des métriques, consultez [Statistiques CloudWatch Amazon pour Amazon EBS](#). Pour plus d'informations sur le suivi de l'état de vos volumes, consultez [EventBridge Événements Amazon pour Amazon EBS](#).

Persistance des données

Un volume EBS est un stockage hors instance qui peut persister indépendamment de la vie d'une instance. Vous continuez à payer pour l'utilisation du volume tant que les données persistent.

Les volumes EBS attachés à une instance en cours d'exécution peuvent se détacher automatiquement de l'instance avec leurs données intactes lorsque l'instance est résiliée, si vous cochez la case Supprimer lors de la résiliation lorsque vous configurez les volumes EBS pour votre instance sur la console EC2. Le volume peut être attaché à une nouvelle instance, ce qui permet une récupération rapide. Si la case Supprimer lors de la résiliation est cochée, le ou les volumes seront supprimés lors de la résiliation de l'instance EC2. Si vous utilisez une EBS-backed instance, vous pouvez arrêter et redémarrer cette instance sans affecter les données stockées dans le volume attaché. Le volume reste attaché pendant le cycle d'arrêt-démarrage. Cela vous permet de traiter et de stocker indéfiniment les données sur votre volume, en utilisant les ressources de traitement et de stockage uniquement lorsque cela est nécessaire. Les données persistent sur le volume jusqu'à ce que ce volume soit explicitement supprimé. Le stockage par blocs physique utilisé par les volumes EBS supprimés est remplacé par des zéros ou des données pseudo-aléatoires cryptographiquement avant d'être alloué à un nouveau volume. Si vous travaillez avec des données sensibles, nous vous recommandons de chiffrer vos données manuellement ou de les stocker sur un volume protégé par Chiffrement Amazon EBS. Pour plus d'informations, consultez [Chiffrement Amazon EBS](#).

Par défaut, le volume EBS racine qui est créé et attaché à une instance au moment du lancement est supprimé lorsque cette instance prend fin. Vous pouvez modifier ce comportement en changeant la valeur de l'indicateur `DeleteOnTermination` en `false` lorsque vous lancez l'instance. En modifiant cette valeur, le volume persiste même après que l'instance ait pris fin, ce qui vous permet de l'attacher à une autre instance.

Par défaut, les volumes EBS supplémentaires qui sont créés et attachés à une instance au moment du lancement ne sont pas supprimés lorsque cette instance prend fin. Vous pouvez modifier ce

comportement en changeant la valeur de l'indicateur `DeleteOnTermination` en `true` lorsque vous lancez l'instance. Cette valeur modifiée entraîne la suppression des volumes lorsque l'instance prend fin.

Chiffrement des données

Pour simplifier le chiffrement des données, vous pouvez créer des volumes EBS chiffrés avec la fonction Chiffrement Amazon EBS. Tous les types de volume EBS prennent en charge le chiffrement. Vous pouvez utiliser des volumes EBS chiffrés pour répondre à un large éventail d'exigences de chiffrement des données au repos pour les *regulated/audited* données et les applications. Le chiffrement Amazon EBS utilise des algorithmes Advanced Encryption Standard 256 bits (AES-256) et une Amazon-managed infrastructure clé. Le chiffrement est effectué sur le serveur qui héberge l'instance EC2, assurant ainsi le chiffrement des données qui se déplacent entre l'instance EC2 et le stockage Amazon EBS. Pour plus d'informations, consultez [Chiffrement Amazon EBS](#).

Le chiffrement Amazon EBS est utilisé AWS KMS keys lors de la création de volumes chiffrés et de tous les instantanés créés à partir de vos volumes chiffrés. La première fois que vous créez un volume EBS chiffré dans une région, une clé KMS AWS gérée par défaut est automatiquement créée pour vous. Cette clé est utilisée pour le chiffrement Amazon EBS, sauf si vous créez et utilisez une clé gérée par le client. La création de votre propre clé gérée par le client vous offre plus de flexibilité, notamment la possibilité de créer, de modifier, de désactiver, de définir des contrôles d'accès et d'auditer les clés de chiffrement utilisées pour protéger vos données. Pour plus d'informations, consultez le [Guide du développeur AWS Key Management Service](#).

Sécurité des données

Les volumes Amazon EBS vous sont présentés comme des périphériques de stockage en mode bloc bruts non formatés. Ces appareils sont des périphériques logiques créés sur l'infrastructure EBS et le service Amazon EBS garantit que les appareils sont logiquement vides (c'est-à-dire que les blocs bruts sont mis à zéro ou contiennent des données pseudo-aléatoires cryptographiques) avant toute utilisation ou réutilisation par un client.

Si vous avez des procédures qui exigent que toutes les données soient effacées à l'aide d'une méthode spécifique, après ou avant utilisation (ou les deux), telles que celles détaillées dans DoD 5220.22-M (National Industrial Security Program Operating Manual) ou NIST 800-88 (Guidelines for Media Sanitization), vous avez la possibilité de le faire sur Amazon EBS. Cette activité de niveau bloc sera reflétée sur le support de stockage sous-jacent du service Amazon EBS.

Instantanés

Amazon EBS donne la possibilité de créer des instantanés (sauvegardes) d'un volume EBS et de copier les données dans le volume sur Amazon S3, où elles sont stockées de façon redondante dans plusieurs zones de disponibilité. Le volume n'a pas besoin d'être attaché à une instance en cours d'exécution pour pouvoir créer un instantané. Alors que vous continuez à écrire des données sur un volume, vous pouvez créer régulièrement un instantané de ce dernier afin de l'utiliser comme base pour de nouveaux volumes. Ces instantanés peuvent être utilisés pour créer plusieurs volumes EBS ou déplacer des volumes entre les zones de disponibilité. Les instantanés de volumes EBS chiffrés sont chiffrés automatiquement.

Lorsque vous créez un volume à partir d'un instantané, celui-ci est une copie exacte du volume initial au moment où l'instantané a été créé. Les volumes EBS qui sont créés à partir d'instantanés chiffrés sont automatiquement chiffrés. En spécifiant éventuellement une zone de disponibilité différente, vous pouvez utiliser cette fonctionnalité pour dupliquer un volume dans cette zone. Les instantanés peuvent être partagés avec des AWS comptes spécifiques ou rendus publics. Lorsque vous créez des instantanés, vous occasionnez des frais dans Amazon S3 en fonction de la taille des données sauvegardées, et non de la taille du volume source. Les instantanés suivants du même volume sont des instantanés incrémentiels. Ils incluent uniquement les données modifiées et nouvelles écrites sur le volume depuis la création du dernier instantané, et la facturation ne concerne que ces données modifiées et nouvelles.

Les instantanés sont des sauvegardes incrémentielles, ce qui signifie que seuls les blocs du volume qui ont changé depuis l'instantané le plus récent sont enregistrés. Si vous avez un volume de 100 Gio de données mais que seulement 5 Gio ont changé depuis votre dernier instantané, seuls ces 5 Gio de données modifiées sont écrits sur Amazon S3. Bien que les instantanés soient enregistrés de manière incrémentielle, le processus de suppression de l'instantané prévoit que vous avez uniquement besoin de conserver l'instantané le plus récent.

Pour vous aider à classer et à gérer vos volumes et instantanés, vous pouvez les étiqueter avec les métadonnées de votre choix.

Pour la sauvegarde automatique vos volumes, vous pouvez utiliser [Amazon Data Lifecycle Manager](#) ou [AWS Backup](#).

Flexibilité

Les volumes EBS acceptent les modifications de configuration en direct en cours de production. Vous pouvez modifier le type de volume, la taille du volume et la capacité IOPS sans interruption de

service. Pour plus d'informations, consultez [Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes](#).

Types de volume Amazon EBS

Amazon EBS fournit les types de volume suivants, qui ont des caractéristiques de performances et des prix différents, ce qui vous permet d'adapter vos performances de stockage et vos coûts en fonction des besoins de vos applications.

Important

Plusieurs facteurs peuvent affecter les performances des volumes EBS, tels que la configuration, les I/O caractéristiques et la charge de travail des instances. Pour utiliser pleinement les IOPS provisionnées sur un volume EBS, utilisez [des instances optimisées pour EBS](#). Pour plus d'informations sur la façon d'exploiter au mieux vos volumes EBS, consultez [Performances volumiques d'Amazon EBS](#).

Pour plus d'informations sur la tarification, consultez [Tarification Amazon EBS](#).

Types de volume

- [Volumes de disque SSD \(solid state drive\)](#)
- [Volumes de disque dur \(HDD\)](#)
- [Volumes de la génération précédente](#)

Volumes de disque SSD (solid state drive)

SSD-backed les volumes sont optimisés pour les charges de travail transactionnelles impliquant des read/write opérations fréquentes de petite I/O taille, où l'attribut de performance dominant est l'IOPS. SSD-backed les types de volumes incluent les SSD à usage général et les SSD IOPS provisionnés. Voici un résumé des cas d'utilisation et des caractéristiques des SSD-backed volumes.

	<u>Volumes SSD à usage général Amazon EBS</u>		<u>Volumes SSD IOPS provisionnés par Amazon EBS</u>	
Type de volume	gp3 ⁶	gp2	io2Bloquer Express	io1
Durabilité	99,8 % - 99,9 % (taux de défaillance annuel de 0,1 % - 0,2 %)		Durabilité de 99,999 % (taux de défaillance annuel de 0,001 %)	Durabilité de 99,8 % - 99,9 % (taux de défaillance annuel de 0,1 % - 0,2 %)
Cas d'utilisation	<ul style="list-style-type: none"> Charges de travail transactionnelles Bureaux virtuels Medium-sized, bases de données à instance unique Low-latency applications interactives Volumes de démarrage Environnements de développement et de test 		Charges de travail nécessitant : <ul style="list-style-type: none"> Latence constante inférieure à la milliseconde avec une latence moyenne inférieure à 500 microsecondes Performance IOPS soutenue Plus de 80 000 IOPS ou 2 000 MiB/s de débit 	<ul style="list-style-type: none"> Charges de travail nécessitant des performances IOPS soutenues ou supérieures à 16,000 IOPS I/O-intensive charges de travail de base de données
Taille du volume	1 Gio à 64 TiB	1 Gio - 16 Tio	4 Gio - 64 Tio	4 Gio - 16 Tio
IOPS maximum	80 000 (25,6 KiB 4 I/O ⁷)	16 000 (16 livres sur I/O ⁴)	256 000 (16 livres sur I/O ⁴)	64 000 (16 livres sur I/O ⁴)

	<u>Volumes SSD à usage général Amazon EBS</u>		<u>Volumes SSD IOPS provision nés par Amazon EBS</u>	
Débit maximal	2 000 MiB/s	250 MiB/s ¹	4 000 MiB/s	1 000 MiB/s ²
Amazon EBS Multi-attach	Non pris en charge		Pris en charge	
Réservations NVMe	Non pris en charge		Pris en charge	Pris en charge
Volume de démarrage	Pris en charge			

¹ La limite de débit est comprise entre 128 MiB/s et 250 MiB/s, selon la taille du volume. Pour plus d'informations, consultez [performance du volume GP2](#). Les volumes créés avant le 3 décembre 2018 et qui n'ont pas été modifiés depuis leur création peuvent ne pas atteindre des performances optimales, sauf si vous [modifiez le volume](#).

² Pour atteindre un débit maximal de 1 000 MiB/s, le volume doit être provisionné avec 64 000 IOPS et il doit être attaché à une instance. [Nitro-based](#) Les volumes créés avant le 6 décembre 2017 et qui n'ont pas été modifiés depuis leur création peuvent ne pas atteindre des performances optimales, sauf si vous [modifiez le volume](#).

³ [Nitro-based instances](#) prennent en charge des volumes provisionnés avec un maximum de 256 000 IOPS. D'autres types d'instances peuvent être connectés à des volumes alloués avec jusqu'à 64 000 IOPS, mais peuvent atteindre 32 000 IOPS.

⁴ Représente la I/O taille requise pour atteindre le maximum d'IOPS dans la limite de débit du volume.

Les volumes ⁵ [io2 Block Express](#) sont conçus pour fournir une latence moyenne inférieure à 500 microsecondes pour des opérations de 16 Ko I/O .

⁶ Sur Outposts, les volumes gp3 prennent en charge des tailles allant jusqu'à 16 TiB, des IOPS jusqu'à 16 000 et un débit allant jusqu'à 1 000. MiB/s

Pour plus d'informations sur les types de SSD-backed volumes, consultez les rubriques suivantes :

- [Volumes SSD à usage général Amazon EBS](#)
- [Volumes SSD IOPS provisionnés par Amazon EBS](#)

Volumes de disque dur (HDD)

HDD-backed les volumes sont optimisés pour les charges de travail de streaming importantes où l'attribut de performance dominant est le débit. Les types de volume HDD incluent les HDD à débit optimisé et les HDD à froid. Voici un résumé des cas d'utilisation et des caractéristiques des HDD-backed volumes.

	Volumes HDD à débit optimisé	Volumes HDD à froid
Type de volume	st1	sc1
Durabilité	99,8 % - 99,9 % (taux de défaillance annuel de 0,1 % - 0,2 %)	
Cas d'utilisation	<ul style="list-style-type: none"> • Big Data • Entrepôts de données • Traitement de fichiers journaux 	<ul style="list-style-type: none"> • Throughput-oriented stockage des données rarement consultées • Scénarios dans lesquels il est important que le coût de stockage soit le plus bas possible
Taille du volume	125 Gio - 16 Tio	
Nombre maximum d'IOPS par volume (1 I/O MiB)	500	250
Débit maximal par volume	500 MiB/s	250 MiB/s

	Volumes HDD à débit optimisé	Volumes HDD à froid
Amazon EBS Multi-attach	Non pris en charge	
Volume de démarrage	Non pris en charge	

Pour de plus amples informations sur les volumes des disques durs (HDD), veuillez consulter [Volumes des disques durs et des disques durs froids optimisés pour le débit Amazon EBS](#).

Volumes de la génération précédente

Les volumes magnétiques (standard) sont des volumes de génération précédente basés sur des disques magnétiques. Ils conviennent aux charges de travail comportant des jeux de données réduits où l'accès aux données est rare et où les performances n'ont pas une importance primordiale. Ces volumes fournissent en moyenne 100 IOPS, avec la possibilité d'émettre en rafale jusqu'à des centaines d'IOPS. Leur taille varie entre 1 GiB et 1 TiB.

Tip

Les volumes magnétiques sont des volumes de génération précédente. Si vous avez besoin de performances ou d'une cohérence des performances supérieures à celles que peuvent fournir les volumes de la génération précédente, nous vous recommandons d'utiliser l'un des types de volumes de la génération actuelle.

Le tableau suivant décrit les types de volume EBS de la génération précédente.

	Magnétique
Type de volume	standard
Cas d'utilisation	Charges de travail où l'accès aux données est occasionnel
Taille du volume	1 GiB-1 TiB

	Magnétique
IOPS maximum par volume	40–200
Débit maximal par volume	40 à 90 MiB/s
Volume de démarrage	Pris en charge

Volumes SSD à usage général Amazon EBS

Les volumes SSD à usage général (gp2 et gp3) sont soutenus par des disques durs à état solide (SSD). Ils constituent un bon compromis en termes de prix et de performances pour un large éventail de charges de travail transactionnelles. Il s'agit notamment des bureaux virtuels, des bases de données à instance unique de taille moyenne, des applications interactives sensibles à la latence, des environnements de développement et de test, ainsi que des volumes de démarrage. Nous recommandons ces volumes pour la plupart des charges de travail.

Amazon EBS propose les types suivants de volumes SSD à usage général :

Types

- [Volumes SSD à usage général \(gp3\)](#)
- [Volumes SSD à usage général \(gp2\)](#)

Volumes SSD à usage général (gp3)

Les volumes SSD à usage général (gp3) sont la dernière génération de volumes SSD à usage général, et le volume SSD le moins cher proposé par Amazon EBS. Ce type de volume permet de fournir le bon équilibre entre le prix et les performances pour la plupart des applications. Il vous permet également de faire évoluer les performances du volume indépendamment de sa taille. Cela signifie que vous pouvez fournir la performance requise sans avoir besoin de fournir une capacité de stockage en mode bloc supplémentaire. En outre, les volumes gp3 offrent un prix par Gio inférieur de 20 % à celui des volumes SSD à usage général (gp2).

Les volumes gp3 offrent une latence à un chiffre en millisecondes et une durabilité des volumes de 99,8 % à 99,9 % avec un taux de défaillance annuel (AFR) inférieur à 0,2 %, ce qui se traduit par un maximum de deux défaillances de volume pour 1 000 volumes en cours d'exécution sur une période d'un an. AWS conçoit des volumes GP3 pour fournir les performances prévues 99 % du temps.

 Tip

Pour les charges de travail sensibles à la latence, nous vous recommandons d'utiliser les volumes io2 Block Express. io2 Les volumes Block Express sont conçus pour fournir une latence moyenne inférieure à 500 microsecondes pour des opérations de 16 Ko I/O . io2 Les volumes Block Express offrent également une meilleure latence pour les valeurs aberrantes que les volumes à usage général, réduisant ainsi de plus de 10 fois la fréquence des I/Os dépassements de 800 microsecondes. Pour plus d'informations, consultez [Volumes Block Express du SSD IOPS \(io2\) provisionnés](#).

Table des matières

- [Performances des volumes gp3](#)
- [Taille du volume gp3](#)
- [Migrer vers gp3 depuis gp2](#)

Performances des volumes gp3

 Tip

Les volumes gp3 n'utilisent pas de performances en rafale. Ils peuvent maintenir indéfiniment leurs meilleures performances en termes d'IOPS provisionnés et de débit.

Performance IOPS

Les volumes gp3 offrent une performance IOPS de base constante de 3 000 IOPS, qui est incluse dans le prix du stockage. Vous pouvez provisionner des IOPS supplémentaires (jusqu'à un maximum de 80 000) moyennant un coût supplémentaire à un ratio de 500 IOPS par GiB de volume. Un maximum d'IOPS peut être provisionné pour des volumes de 160 GiB ou plus (500 IOPS par GiB × 160 GiB = 80 000 IOPS).

Performances de débit

Les volumes gp3 offrent un débit de référence constant de 125 MiB/s, qui est inclus dans le prix du stockage. Vous pouvez provisionner un débit supplémentaire (jusqu'à un maximum de 2 000 MiB/s) moyennant un coût supplémentaire à un ratio de 0,25 MiB/s par IOPS provisionnée. Le débit maximal

peut être provisionné à 8 000 IOPS ou plus et à 16 GiB ou plus (8 000 IOPS × 0,25 MiB/s par IOPS = 2 000). MiB/s

Note

Sur Outposts, les volumes gp3 prennent en charge des tailles allant jusqu'à 16 TiB, des IOPS jusqu'à 16 000 et un débit allant jusqu'à 1 000. MiB/s

Taille du volume gp3

La taille d'un volume gp3 peut varier de 1 GiB à 64 TiB.

Migrer vers gp3 depuis gp2

Si vous utilisez actuellement des volumes gp2, vous pouvez migrer vos volumes vers gp3 en utilisant les opérations [Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes](#). Vous pouvez utiliser les opérations Amazon EBS Elastic Volumes pour modifier le type de volume, les IOPS et le débit de vos volumes existants sans interrompre vos instances Amazon EC2. Lorsque vous utilisez la console pour créer un volume ou pour créer une AMI à partir d'un instantané, le type de volume sélectionné par défaut est le stockage SSD à usage général gp3. Dans les autres cas, gp2 est sélectionné par défaut. Dans ces cas, vous pouvez sélectionner gp3 comme type de volume au lieu d'utiliser gp2.

Pour savoir combien vous pouvez économiser en migrant vos volumes gp2 vers gp3, utilisez le [calculateur d'économies de coûts de migration de gp2 à gp3 d'Amazon EBS](#).

Volumes SSD à usage général (gp2)

Ils offrent un stockage économique idéal pour un large éventail de charges de travail transactionnelles. Avec les volumes gp2, les performances évoluent avec la taille du volume.

Tip

Les volumes gp3 sont la dernière génération de volumes SSD à usage général. Ils offrent une évolution des performances plus prévisible et des prix jusqu'à 20 % inférieurs à ceux des volumes gp2. Pour plus d'informations, consultez [Volumes SSD à usage général \(gp3\)](#). Pour savoir combien vous pouvez économiser en migrant vos volumes gp2 vers gp3, utilisez le [calculateur d'économies de coûts de migration de gp2 à gp3 d'Amazon EBS](#).

gp2les volumes offrent une latence d'une milliseconde à un chiffre et une durabilité des volumes de 99,8 % à 99,9 % avec un taux de défaillance annuel (AFR) inférieur à 0,2 %, ce qui se traduit par un maximum de deux défaillances de volume pour 1 000 volumes en cours d'exécution sur une période d'un an. AWS conçoit des gp2 volumes de manière à fournir les performances prévues 99 % du temps.

Table des matières

- [performance du volume GP2](#)
- [taille du volume gp2](#)

performance du volume GP2

Performance IOPS

Les performances IOPS de base évoluent de façon linéaire entre un minimum de 100 et un maximum de 16 000, à raison de 3 IOPS par Gio de taille de volume. Les performances IOPS sont provisionnées comme suit :

- Les volumes de 33,33 Gio et moins sont provisionnés avec un minimum de 100 IOPS.
- Les volumes supérieurs à 33,33 Gio sont provisionnés avec 3 IOPS par Gio de taille de volume jusqu'au maximum de 16 000 IOPS, qui est atteint à 5 334 Gio (3 X 5 334).
- Les volumes de 5 334 Gio et plus sont provisionnés avec 16 000 IOPS.

Les volumes gp2 de moins de 1 Tio (et qui sont provisionnés avec moins de 3 000 IOPS) peuvent atteindre 3 000 IOPS en cas de besoin pendant une période prolongée. La capacité d'un volume à exploser est déterminée par les I/O crédits. Lorsque I/O la demande est supérieure aux performances de base, le volume dépense des I/O crédits pour atteindre le niveau de performance requis (jusqu'à 3 000 IOPS). En cas de rafale, les I/O crédits ne sont pas accumulés et sont dépensés au taux d'IOPS utilisé au-dessus des IOPS de référence (taux de dépenses = IOPS en rafale - IOPS de référence). Plus un volume accumule de I/O crédits, plus il peut maintenir ses performances en rafale. Vous pouvez calculer la durée des rafales comme suit :

$$\text{Burst duration} = \frac{(\text{I/O credit balance})}{(\text{Burst IOPS}) - (\text{Baseline IOPS})}$$

Lorsque I/O la demande atteint le niveau de performance de base ou inférieur, le volume commence à gagner des I/O crédits à raison de 3 I/O crédits par GiB de volume par seconde. Les volumes ont une limite d'accumulation de I/O crédits de 5,4 millions de I/O crédits, ce qui est suffisant pour maintenir les performances de rafale maximales de 3 000 IOPS pendant au moins 30 minutes.

 Note

Chaque volume reçoit un solde I/O créditeur initial de 5,4 millions de I/O crédits, ce qui permet un cycle de démarrage initial rapide pour les volumes de démarrage et une bonne expérience de démarrage pour les autres applications.

Le tableau suivant répertorie des exemples de tailles de volume et les performances de base associées au volume, la durée de rafale (lorsque vous commencez avec 5,4 millions de I/O crédits) et le temps nécessaire pour recharger un solde de I/O crédits vide.

Taille du volume (GiB)	Performances de base (IOPS)	Durée de performances en rafale à 3 000 IOPS (en secondes)	Temps nécessaire pour recharger un solde de crédits vide (en secondes)
1 à 33,33	100	1,862	54 000
100	300	2 000	18 000
334 (taille minimale pour débit maximal)	1 002	2 703	5 389
750	2 250	7 200	2 400
1 000	3 000	N/A*	N/A*
5 334 (taille minimale pour IOPS maximum) et plus	16,000	N/A*	N/A*

* Les performances de base du volume dépassent les celles en rafale maximales.

Vous pouvez surveiller le solde I/O créditeur d'un volume à l'aide de la `BurstBalance` métrique Amazon EBS dans Amazon CloudWatch. Cette métrique indique le pourcentage de I/O crédits gp2 restants. Pour plus d'informations, consultez [I/O Caractéristiques et surveillance d'Amazon EBS](#). Vous pouvez définir une alarme qui vous notifie lorsque la valeur `BurstBalance` tombe à un certain niveau. Pour plus d'informations, consultez la section [Création d' CloudWatch alarmes](#).

Performances de débit

gp2les volumes fournissent un débit compris entre 128 MiB/s et 250 MiB/s, selon la taille du volume. Les performances de débit sont provisionnées comme suit :

- Les volumes inférieurs ou égaux à 170 GiB fournissent un débit maximal de 128 Go MiB/s.
- Les volumes supérieurs à 170 GiB mais inférieurs à 334 GiB peuvent atteindre un débit maximal de 250. MiB/s
- Les volumes de 334 GiB et plus en fournissent 250 MiB/s.

Le débit d'un gp2 volume peut être calculé à l'aide de la formule suivante, jusqu'à la limite de débit de 250 MiB/s :

$$\text{Throughput in MiB/s} = \text{IOPS performance} \times \text{I/O size in KiB} / 1,024$$

taille du volume gp2

La taille des volumes gp2 peut aller de 1 Gio à 16 Tio. N'oubliez pas que les performances du volume évoluent de façon linéaire avec sa taille.

Volumes SSD IOPS provisionnés par Amazon EBS

Les volumes SSD IOPS provisionnés sont soutenus par des disques durs à l'état solide (SSD). Il s'agit des volumes de stockage Amazon EBS les plus performants conçus pour les charges de travail critiques et gourmandes en débit nécessitant une faible latence. IOPS-intensive Les volumes SSD IOPS provisionnés fournissent leurs performances d'IOPS provisionnés 99,9 % du temps.

Amazon EBS propose deux types de volumes SSD IOPS provisionnés :

- [Volumes Block Express du SSD IOPS \(io2\) provisionnés](#)
- [Volumes IOPS SSD \(io1\) provisionnés](#)

Volumes Block Express du SSD IOPS (**io2**) provisionnés

Les volumes Block Express io2 reposent sur la nouvelle génération d'architecture de serveur de stockage Amazon EBS. Il a été conçu dans le but de répondre aux exigences de performances des applications I/O intensives les plus exigeantes qui s'exécutent sur [des instances basées sur le système](#) Nitro. Avec une durabilité maximale et une latence minimale, Block Express est idéal pour exécuter des charges de travail stratégiques et exigeantes en termes de performances, telles qu'Oracle, SAP HANA, Microsoft SQL Server et SAS Analytics.

L'architecture Block Express augmente les performances et l'évolutivité des volumes io2. Les serveurs Block Express communiquent avec les [Nitro-based instances](#) à l'aide du protocole réseau Scalable Reliable Datagram (SRD). Cette interface est implémentée dans la carte Nitro dédiée à la I/O fonction Amazon EBS sur le matériel hôte de l'instance. Il minimise les I/O retards et les variations de latence (gigue du réseau), ce qui garantit des performances plus rapides et plus cohérentes pour vos applications.

Les volumes io2 Block Express sont conçus pour offrir une durabilité de 99,999 % avec un taux de défaillance annuel (AFR) ne dépassant pas 0,001 %, ce qui se traduit par une défaillance de volume unique pour 100 000 volumes exécutés sur une période d'un an. io2 Les volumes Block Express sont adaptés aux charges de travail qui bénéficient d'un volume unique offrant une latence constante inférieure à la milliseconde et prenant en charge des IOPS et un débit supérieurs à ceux des volumes gp3.

Lorsqu'ils sont attachés à [Nitro-based des instances](#), les volumes io2 Block Express sont conçus pour fournir une latence moyenne inférieure à 500 microsecondes pour des opérations de 16 Ko I/O . io2 Les volumes Block Express offrent également une meilleure latence pour les valeurs aberrantes que les volumes à usage général, réduisant ainsi de plus de 10 fois la fréquence des I/Os dépassements de 800 microsecondes.

Rubriques

- [Considérations](#)
- [Performance](#)

Considérations

- io2 Les volumes Block Express sont disponibles dans toutes les AWS régions, y compris les AWS GovCloud (US) régions et les régions de Chine.

- Au 30 avril 2025, tous les volumes nouveaux et créés précédemment étaient io2 des volumes io2 Block Express.
- [Nitro-based les instances](#) prennent en charge des volumes provisionnés avec un maximum de 256 000 IOPS. D'autres types d'instances peuvent être connectés à des volumes alloués avec jusqu'à 64 000 IOPS, mais peuvent atteindre 32 000 IOPS.

Performance

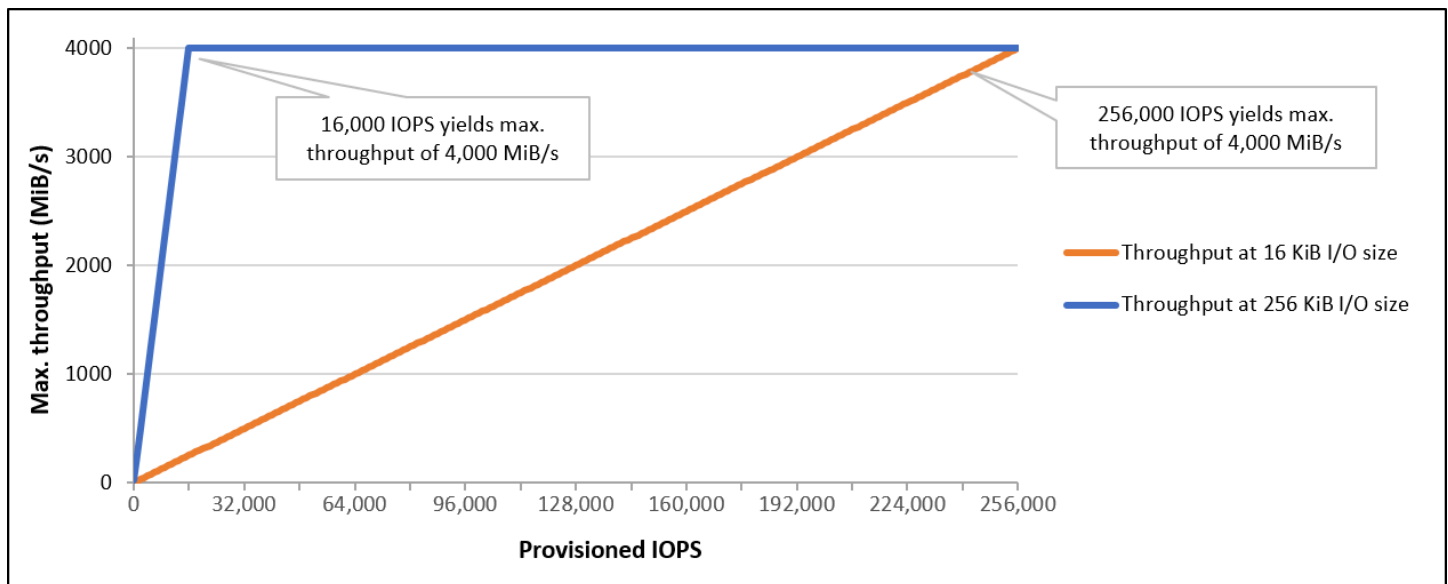
io2Les volumes Block Express présentent les caractéristiques suivantes :

- Latence moyenne inférieure à 500 microsecondes pour une taille de 16 Ko I/O . Meilleure latence des valeurs aberrantes par rapport aux volumes à usage général, réduisant de plus de 10 fois la fréquence des I/Os dépassements de 800 microsecondes.
- Capacité de stockage jusqu'à 64 TiB (65 536 GiB).
- IOPS provisionnées jusqu'à 256 000, avec un IOPS:GiB ratio de 1 000:1. Les IOPS maximaux peuvent être provisionnés avec des volumes de 256 Gio et plus ($1\,000\text{ IOPS} \times 256\text{ Gio} = 256\,000\text{ IOPS}$).

Note

Vous pouvez atteindre 256 000 IOPS avec [Nitro-based les instances](#). Dans d'autres cas, vous pouvez atteindre jusqu'à 32 000 IOPS.

- Débit de volume allant jusqu'à 4 000 MiB/s. Le débit évolue proportionnellement à un taux de 0,256 MiB/s par IOPS provisionnée. Le débit maximal peut être atteint à 16 000 IOPS ou plus.



Volumes IOPS SSD (io1) provisionnés

Les volumes IOPS SSD (io1) provisionnés sont conçus pour répondre aux besoins des charges de travail, en particulier des I/O-intensive charges de travail de base de données, qui sont sensibles aux performances et à la cohérence du stockage. Les volumes SSD IOPS provisionnés utilisent un taux d'IOPS régulier, que vous spécifiez lors de la création du volume, et Amazon EBS fournit les performances provisionnées 99,9 % du temps.

Les volumes io1 sont conçus pour offrir une durabilité de 99,8 à 99,99 % avec un taux de défaillance annuel (AFR) ne dépassant pas 0,2 %, ce qui se traduit par un maximum de deux défaillances de volume pour 1 000 volumes exécutés sur une période d'un an.

Les volumes io1 sont disponibles pour tous les types d'instances Amazon EC2.

Performance

La taille des volumes io1 peut aller de 4 Gio à 16 Tio, et vous pouvez allouer de 100 à 64 000 IOPS par volume. Le rapport maximal entre les volumes IOPS provisionnés et le volume demandé (en Gio) est de 50 pour 1. Par exemple, un volume io1 de 100 Gio peut être allouée avec jusqu'à 5 000 IOPS.

Les IOPS maximum peuvent être allouées pour les volumes de 1 280 Gio ou plus ($50 \times 1\,280 \text{ Gio} = 64\,000 \text{ IOPS}$).

- Les volumes `io1` provisionnés avec un maximum de 32 000 IOPS prennent en charge une I/O taille maximale de 256 Ko et fournissent jusqu'à 500 MiB/s de débit. Avec la I/O taille maximale, le débit de pointe est atteint à 2 000 IOPS.
- Les volumes `io1` alloués avec plus de 32 000 IOPS (jusqu'à 64 000 IOPS maximum) génèrent une augmentation linéaire du débit suivant un débit de 16 Kio par I/O par IOPS provisionné. Par exemple, un volume provisionné avec 48 000 IOPS peut prendre en charge jusqu'à 750 MiB/s de débit (16 Ko par IOPS provisionnée × 48 000 IOPS provisionnées = 750). MiB/s
- Pour atteindre le débit maximal de 1 000 MiB/s, un volume doit être provisionné avec 64 000 IOPS (16 Ko par IOPS provisionnées × 64 000 IOPS provisionnées = 1 000). MiB/s
- Vous pouvez atteindre jusqu'à 64 000 IOPS uniquement sur les [Nitro-based instances](#). Dans d'autres cas, vous pouvez atteindre jusqu'à 32 000 IOPS.

. Le graphique suivant illustre ces performances :



Votre expérience par I/O latence dépend des IOPS provisionnées et de votre profil de charge de travail. Pour bénéficier d' I/O une expérience de latence optimale, assurez-vous de configurer les IOPS en fonction du I/O profil de votre charge de travail.

Volumes des disques durs et des disques durs froids optimisés pour le débit Amazon EBS

Les HDD-backed volumes fournis par Amazon EBS entrent dans les catégories suivantes :

- HDD à débit optimisé — HDD conçu pour les charges de travail à débit élevé fréquemment consultées.

- Disque dur froid : le disque dur le moins cher conçu pour les charges de travail les moins fréquemment utilisées.

Rubriques

- [Restrictions de débit par instance](#)
- [Volumes HDD à débit optimisé](#)
- [Volumes HDD à froid](#)
- [Considérations relatives aux performances lors de l'utilisation de volumes HDD](#)
- [Surveiller l'équilibre du compartiment en rafales pour les volumes](#)

Restrictions de débit par instance

Le débit des volumes st1 et sc1 est toujours déterminé par la limite suivante la plus faible:

- Limites de débit du volume
- Limites de débit de l'instance

Comme pour tous les volumes Amazon EBS, nous vous recommandons de sélectionner une instance EBS-optimized EC2 appropriée afin d'éviter les goulots d'étranglement du réseau.

Volumes HDD à débit optimisé

Les volumes HDD à débit optimisé (st1) offrent un stockage magnétique économique qui définit les performances en termes de débit plutôt que d'IOPS. Ce type de volume convient aux charges de travail séquentielles et volumineuses comme Amazon EMR, ETL, les entrepôts de données et le traitement des journaux. Les volumes st1 démarrables ne sont pas pris en charge.

Les volumes HDD à débit optimisé (st1) sont similaires aux volumes HDD à froid (sc1), mais ils sont conçus pour prendre en charge les données fréquemment consultées.

Note

Ce type de volume est optimisé pour les charges de travail impliquant de grandes charges de travail séquentielles I/O, et nous recommandons aux clients dont les charges de travail effectuent une utilisation limitée et aléatoire I/O ou. [Volumes SSD à usage général Amazon](#)

[EBS Volumes SSD IOPS provisionnés par Amazon EBS](#) Pour plus d'informations, consultez [Inefficacité du petit disque read/writes dur](#).

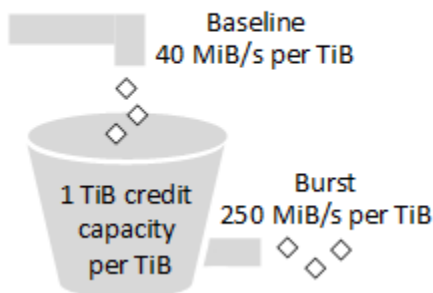
Les volumes de disque dur (st1) à débit optimisé attachés aux EBS-optimized instances sont conçus pour offrir des performances constantes, fournissant au moins 90 % des performances de débit attendues 99 % du temps au cours d'une année donnée.

Crédits de débit et performances en rafale

À l'instar de gp2, st1 utilise un modèle de transmission de compartiment en rafales pour assurer les performances. La taille du volume détermine le débit de base du volume, qui correspond à la vitesse à laquelle le volume accumule des crédits de débit. La taille du volume détermine également le débit de transmission en rafales du volume, qui correspond à la vitesse à laquelle vous pouvez utiliser des crédits lorsqu'ils sont disponibles. Les gros volumes ont un débit de base et de transmission en rafales plus élevé. Plus votre volume est crédité, plus il peut durer longtemps I/O au niveau de la rafale.

Le schéma suivant illustre le comportement du compartiment en rafales pour st1.

ST1 burst bucket



Sous réserve de la limite de débit et de crédits, le débit disponible d'un volume st1 est exprimé par la formule suivante :

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Pour un st1 volume de 1 TiB, le débit en rafale est limité à 250 MiB/s, le compartiment se remplit de crédits à 40 MiB/s et il peut contenir jusqu'à 1 TiB-worth crédit.

Les volumes plus importants font évoluer ces limites de manière linéaire, le débit étant plafonné à un maximum de 500. MiB/s Une fois le seau épuisé, le débit est limité au taux de référence de 40 MiB/s par TiB.

Sur des volumes allant de 0,125 TiB à 16 TiB, le débit de base varie de 5 MiB/s à un plafond de 500 MiB/s, qui est atteint à 12,5 TiB comme suit :

$$12.5 \text{ TiB} \times \frac{40 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

Le débit de rafale varie de 31 MiB/s à un plafond de 500 MiB/s, qui est atteint à 2 TiB comme suit :

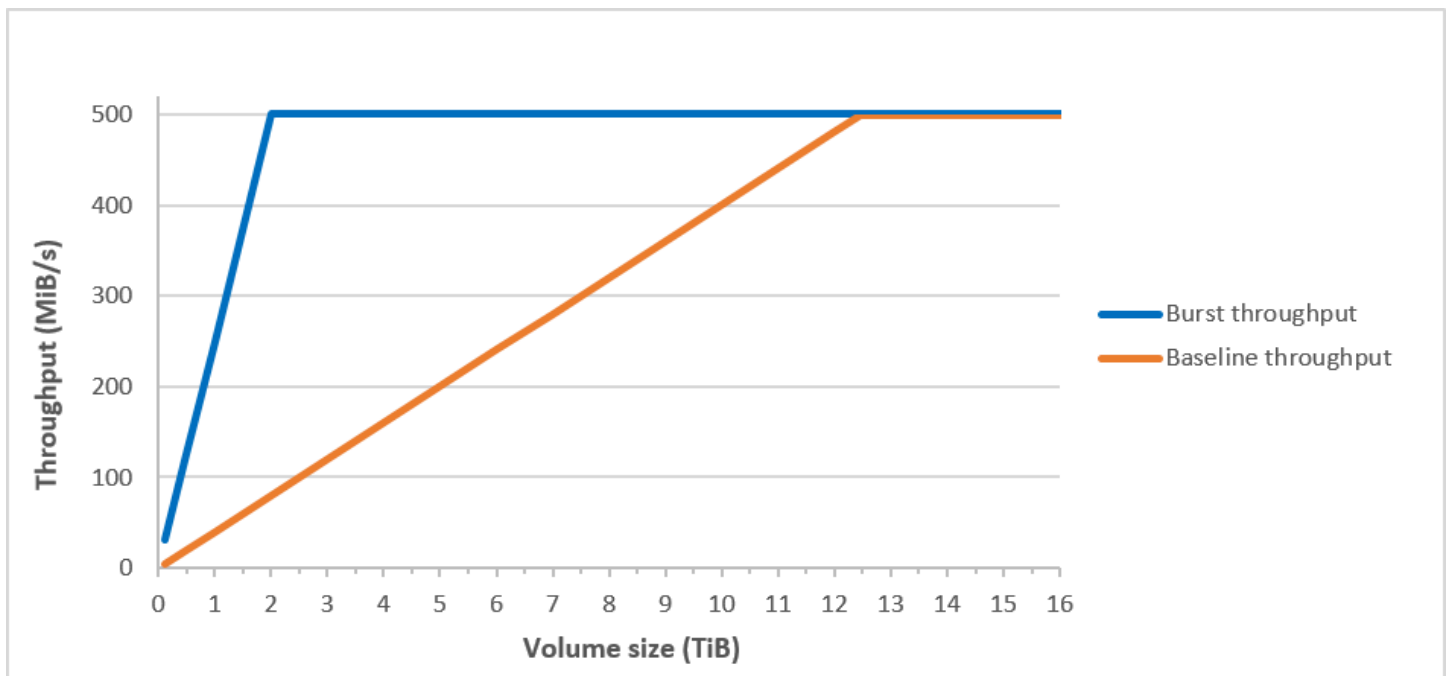
$$2 \text{ TiB} \times \frac{250 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

Le tableau suivant indique l'ensemble des valeurs de base en matière de débit et de transmission en rafales pour st1.

Taille du volume (TiB)	Débit de base ST1 () MiB/s	Débit de rafale ST1 () MiB/s
0.125	5	31
0,5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500

Taille du volume (TiB)	Débit de base ST1 () MiB/s	Débit de rafale ST1 () MiB/s
11	440	500
12	480	500
12,5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

Le schéma suivant illustre le tableau de valeurs sous forme de tracé :



Note

Lorsque vous créez un instantané d'un volume HSS à débit optimisé (st1), les performances peuvent diminuer jusqu'à la valeur de référence du volume pendant que l'instantané est en cours de création.

Pour plus d'informations sur l'utilisation de CloudWatch mesures et d'alarmes pour surveiller l'équilibre de votre seau en cas de rupture, consultez [Surveiller l'équilibre du compartiment en rafales pour les volumes](#).

Volumes HDD à froid

Les volumes HDD à froid (sc1) offrent un stockage magnétique économique qui définit les performances en termes de débit plutôt que d'IOPS. Avec une limite de débit inférieure à celle des volumes st1, sc1 convient aux charges de travail séquentielles et volumineuses dont les données sont légères. Si vous n'avez pas besoin d'accéder souvent à vos données et si vous cherchez à réaliser des économies, sc1 fournit un stockage de bloc économique. Les volumes sc1 démarrables ne sont pas pris en charge.

Les volumes HDD à froid (sc1) sont similaires aux volumes HDD à débit optimisé (st1), mais ils sont conçus pour prendre en charge les données consultées de manière occasionnelle.

Note

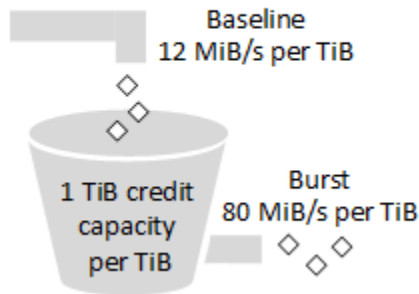
Ce type de volume est optimisé pour les charges de travail impliquant de grandes charges de travail séquentielles I/O, et nous recommandons aux clients dont les charges de travail effectuent une utilisation limitée et aléatoire I/O ou. [Volumes SSD à usage général Amazon EBS](#) [Volumes SSD IOPS provisionnés par Amazon EBS](#) Pour plus d'informations, consultez [Inefficacité du petit disque read/writes dur](#).

Les volumes Cold HDD (sc1) attachés aux EBS-optimized instances sont conçus pour offrir des performances constantes, fournissant au moins 90 % des performances de débit attendues 99 % du temps au cours d'une année donnée.

Crédits de débit et performances en rafale

À l'instar de gp2, sc1 utilise un modèle de transmission de compartiment en rafales pour assurer les performances. La taille du volume détermine le débit de base du volume, qui correspond à la vitesse à laquelle le volume accumule des crédits de débit. La taille du volume détermine également le débit de transmission en rafales du volume, qui correspond à la vitesse à laquelle vous pouvez utiliser des crédits lorsqu'ils sont disponibles. Les gros volumes ont un débit de base et de transmission en rafales plus élevé. Plus votre volume est crédité, plus il peut durer longtemps I/O au niveau de la rafale.

SC1 burst bucket



Sous réserve de la limite de débit et de crédits, le débit disponible d'un volume sc1 est exprimé par la formule suivante :

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Pour un sc1 volume de 1 TiB, le débit en rafale est limité à 80 MiB/s, le compartiment se remplit de crédits à 12 MiB/s et il peut contenir jusqu'à 1 TiB-worth crédit.

Les volumes plus importants font évoluer ces limites de manière linéaire, le débit étant plafonné à un maximum de 250. MiB/s Une fois le seau épuisé, le débit est limité au taux de référence de 12 MiB/s par TiB.

Sur des volumes allant de 0,125 TiB à 16 TiB, le débit de base varie de 1,5 MiB/s à un maximum de 192 MiB/s, qui est atteint à 16 TiB comme suit :

$$16 \text{ TiB} \times \frac{12 \text{ MiB/s}}{1 \text{ TiB}} = 192 \text{ MiB/s}$$

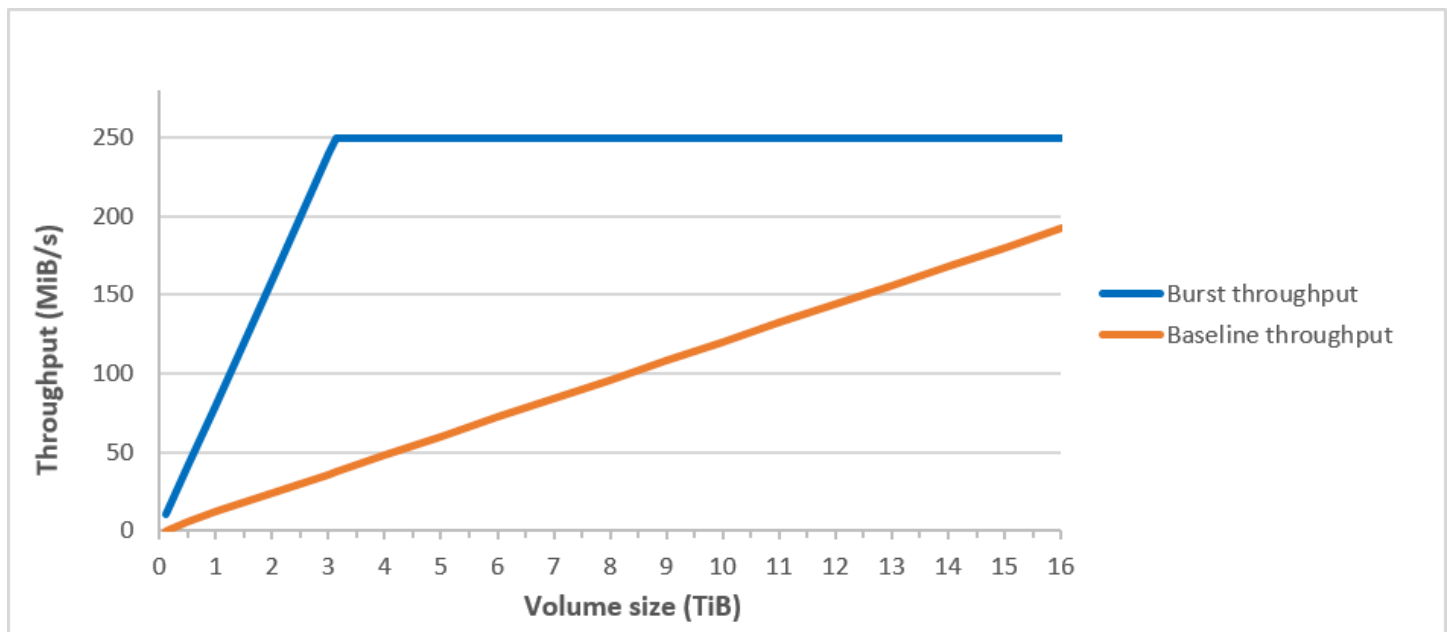
Le débit de rafale varie de 10 MiB/s à un plafond de 250 MiB/s, qui est atteint à 3,125 TiB comme suit :

$$3.125 \text{ TiB} \times \frac{80 \text{ MiB/s}}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

Le tableau suivant indique l'ensemble des valeurs de base en matière de débit et de transmission en rafales pour sc1:

Taille du volume (TiO)	Débit de base SC1 () MiB/s	Débit en rafale SC1 () MiB/s
0.125	1.5	10
0,5	6	40
1	12	80
2	24	160
3	36	240
3,125	37,5	250
4	48	250
5	60	250
6	72	250
7	84	250
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250
16	192	250

Le schéma suivant illustre le tableau de valeurs sous forme de tracé :



Note

Lorsque vous créez un instantané d'un volume HDD à froid (sc1), les performances peuvent diminuer jusqu'à la valeur de référence du volume pendant que l'instantané est en cours de création.

Pour plus d'informations sur l'utilisation de CloudWatch mesures et d'alarmes pour surveiller l'équilibre de votre seau en cas de rupture, consultez [Surveiller l'équilibre du compartiment en rafales pour les volumes](#).

Considérations relatives aux performances lors de l'utilisation de volumes HDD

Pour des performances de débit optimales avec les volumes HDD, planifiez vos charges de travail en gardant à l'esprit les éléments suivants.

Comparaison des volumes HDD à débit optimisé et des volumes HDD à froid

Les tailles de compartiment st1 et sc1 varient selon la taille du volume, et un compartiment complet contient assez de jetons pour une analyse complète du volume. Cependant, l'analyse des volumes st1 et sc1 de plus grande taille est plus longue en raison des limites de débit par instance et par volume. Les volumes attachés à des instances plus petites sont limités par le débit par instance plutôt que par les limites de débit de st1 ou sc1.

Les deux `st1` `sc1` sont conçus pour garantir des performances constantes de 90 % du débit en rafale 99 % du temps. Non-compliant les périodes sont distribuées de manière approximativement uniforme, ciblant 99 % du débit total attendu chaque heure.

En général, les durées d'analyse sont exprimées par cette formule :

$$\frac{\text{Volume size}}{\text{Throughput}} = \text{Scan time}$$

Par exemple, en prenant en compte les garanties en matière de cohérence des performances et les autres optimisations, un client `st1` avec un volume de 5 Tio effectue généralement une analyse complète du volume en 2,91 à 3,27 heures.

- Durée d'analyse optimale

$$\frac{5 \text{ TiB}}{500 \text{ MiB/s}} = \frac{5 \text{ TiB}}{0.00047684 \text{ TiB/s}} = 10,486 \text{ seconds} = 2.91 \text{ hours}$$

- Durée d'analyse maximum

$$\frac{2.91 \text{ hours}}{(0.90)(0.99)} = 3.27 \text{ hours}$$

(0.90)(0.99) <-- From expected performance of 90% of burst 99% of the time

De même, un client `sc1` avec un volume de 5 Tio effectue généralement une analyse complète du volume en 5,83 à 6,54 heures.

- Durée d'analyse optimale

$$\frac{5 \text{ TiB}}{250 \text{ MiB/s}} = \frac{5 \text{ TiB}}{0.000238418 \text{ TiB/s}} = 20972 \text{ seconds} = 5.83 \text{ hours}$$

- Durée d'analyse maximum

$$\frac{5.83 \text{ hours}}{} = 6.54 \text{ hours}$$

(0.90)(0.99)

Le tableau suivant illustre les durées d'analyse idéales pour les volumes de différentes tailles, en supposant que les compartiments sont complets et que le débit d'instance est suffisant.

Taille du volume (Tio)	Durée d'analyse avec transmission en rafales pour ST1 (en heures)*	Durée d'analyse avec transmission en rafales pour SC1 (en heures)*
1	1,17	3,64
2	1,17	3,64
3	1,75	3,64
4	2,33	4,66
5	2,91	5,83
6	3,50	6,99
7	4,08	8,16
8	4,66	9,32
9	5,24	10,49
10	5,83	11,65
11	6,41	12,82
12	6,99	13,98
13	7,57	15,15
14	8,16	16,31
15	8,74	17,48
16	9,32	18,64

* Ces temps de numérisation supposent une profondeur de file d'attente moyenne (arrondie au nombre entier le plus proche) de quatre ou plus lors de l'exécution de 1 Mo de séquentiel I/O.

Par conséquent, si votre charge de travail axée sur le débit doit effectuer des analyses rapidement (jusqu'à 500 MiB/s) ou nécessite plusieurs analyses complètes par jour, utilisez. `st1` Si vous optimisez les coûts, que vos données sont rarement consultées et que vous n'avez pas besoin de plus MiB/s de 250 % de performances de numérisation, utilisez. `sc1`

Inefficacité du petit disque read/writes dur

Le modèle de performance pour `st1` et les `sc1` volumes est optimisé pour les charges de travail séquentielles I/Os, privilégiant les charges de travail à haut débit, offrant des performances acceptables sur les charges de travail avec des IOPS et un débit mixtes, et décourageant les charges de travail peu aléatoires. I/O

Par exemple, une I/O demande de 1 Mio ou moins est considérée comme un crédit de 1 MiB I/O . Cependant, s'ils I/Os sont séquentiels, ils sont fusionnés en I/O blocs de 1 MiB et ne comptent que comme un crédit de 1 I/O MiB.

Surveiller l'équilibre du compartiment en rafales pour les volumes

Vous pouvez surveiller le niveau du compartiment en rafale `st1` et les `sc1` volumes à l'aide de la `BurstBalance` métrique Amazon EBS disponible sur Amazon CloudWatch. Cette métrique indique les crédits de débit restants pour `st1` et `sc1` dans le compartiment en rafale. Pour plus d'informations sur la `BurstBalance` métrique et les autres métriques associées I/O, consultez [I/O Caractéristiques et surveillance d'Amazon EBS](#). CloudWatch vous permet également de définir une alarme qui vous avertit lorsque la `BurstBalance` valeur tombe à un certain niveau. Pour plus d'informations, consultez la section [Création d' CloudWatch alarmes](#).

Contraintes de volume Amazon EBS

La taille d'un volume Amazon EBS est limitée par la physique et l'arithmétique du stockage de données par blocs, ainsi que par les décisions d'implémentation des concepteurs de systèmes d'exploitation et de systèmes de fichiers. AWS impose des limites supplémentaires à la taille des volumes afin de garantir la fiabilité de ses services.

Les sections suivantes décrivent les facteurs les plus importants qui limitent la taille utilisable d'un volume EBS et fournissent des recommandations pour configurer vos volumes EBS.

Sommaire

- [Capacité de stockage](#)
- [Limitations de service](#)
- [Schémas de partitionnement](#)
- [Tailles des blocs de données](#)

Capacité de stockage

Le tableau suivant résume les capacités de stockage théoriques et implémentées des systèmes de fichiers les plus courants sur Amazon EBS, en supposant une taille de bloc de 4 096 octets.

Schéma de partitionnement	Nombre max de blocs adressables	Taille max théorique (blocs x taille de blocs)	Taille max implémentée Ext4*	Taille max implémentée XFS**	Taille max implémentée NTFS	Nombre max pris en charge par EBS
MBR	2 ³²	2 TiO	2 TiO	2 TiO	2 TiO	2 TiO
GPT	2 ⁶⁴	64 ZiO	1 EiO = 1024 ² TiO (50 TiO certifiés sur RHEL7)	500 TiO (certifiés sur RHEL7)	256 TiO	64 TiB †

* [Ext4 Howto](#) et [Quelles sont les limites de taille des fichiers et du système pour Red Hat Enterprise Linux ?](#)

** [Quelles sont les limites de taille des fichiers et du système pour Red Hat Enterprise Linux ?](#)

† Les volumes Block Express io2 prennent en charge jusqu'à 64 TiB pour les partitions GPT. Pour plus d'informations, consultez [Volumes Block Express du SSD IOPS \(io2\) provisionnés](#).

Limitations de service

Amazon EBS extrait le stockage distribué massivement d'un centre de données sur des disques durs virtuels. Pour un système d'exploitation installé sur une instance EC2, un volume EBS attaché

semble être un disque dur physique contenant des secteurs disque de 512 octets. Le système d'exploitation gère l'allocation des blocs de données (ou clusters) sur ces secteurs virtuels au moyen de ses utilitaires de gestion de stockage. L'allocation est conforme à un schéma de partitionnement de volume, comme un MBR (enregistrement de démarrage principal) ou GPT (table de partition GUID), et dans les capacités du système de fichiers installé (ext4, NTFS, etc.).

EBS n'est pas conscient des données contenues dans ses secteurs disque virtuels ; il s'assure uniquement de l'intégrité des secteurs. Cela signifie que AWS les actions et les actions du système d'exploitation sont indépendantes les unes des autres. Lorsque vous sélectionnez une taille de volume, soyez conscient des capacités et des limites de chacune, comme dans les cas suivants :

- A l'heure actuelle, la taille de volume maximal pris en charge par EBS est de 64 TiB. Cela signifie que vous pouvez créer un volume EBS pouvant atteindre 64 TiB. Toutefois, le fait que le système d'exploitation reconnaisse ou non l'ensemble de cette capacité dépend de ses propres caractéristiques de conception et de la façon dont le volume est partitionné.
- Les volumes de démarrage doivent utiliser le schéma de partitionnement MBR ou GPT. L'AMI à partir de laquelle vous lancez une instance détermine le mode de démarrage, puis le schéma de partition utilisé pour le volume de démarrage.

Avec le MBR, les volumes de démarrage sont limités à 2 TiB.

Avec GPT, les volumes de démarrage peuvent atteindre une taille de 64 TiB lorsqu'ils sont utilisés avec le mode de démarrage GRUB2 (Linux) ou UEFI (Windows).

Pour plus d'informations, consultez [Mettre un volume Amazon EBS à disposition pour utilisation](#).

- Non-boot les volumes de 2 TiB (2 048 GiB) ou plus doivent utiliser une table de partition GPT pour accéder à l'intégralité du volume.

Schémas de partitionnement

Parmi les autres impacts, le schéma de partitionnement détermine le nombre de blocs de données logiques pouvant être traités de manière unique sur un seul volume. Pour plus d'informations, consultez [Tailles des blocs de données](#). Les schémas de partitionnement communs utilisés sont MBR (enregistrement de démarrage principal) et GPT (table de partition GUID). Les différences importantes entre ces schémas peuvent être résumées comme suit.

MBR

MBR utilise une structure de données 32 bits pour stocker les adresses de blocs. Autrement, chaque bloc de données est mappé à l'un des 2^{32} entiers possibles. La taille maximale adressable d'un volume est fournie par la formule suivante :

$$2^{32} \times \text{Block size}$$

La taille des blocs des volumes MBR est limitée par convention à 512 octets. Par conséquent :

$$2^{32} \times 512 \text{ bytes} = 2 \text{ TiB}$$

Les solutions d'ingénierie visant à augmenter cette limite de 2 TiB pour les volumes MBR n'ont pas été adoptées largement dans le secteur. Par conséquent, Linux et Windows ne détectent jamais un volume MBR comme étant supérieur à 2 TiB, même s'il AWS indique que sa taille est supérieure.

GPT

GPT utilise une structure de données 64 bits pour stocker les adresses de blocs. Autrement, chaque bloc de données est mappé à l'un des 2^{64} entiers possibles. La taille maximale adressable d'un volume est fournie par la formule suivante :

$$2^{64} \times \text{Block size}$$

La taille des blocs des volumes GPT est limitée communément à 4 096 octets. Par conséquent :

$$\begin{aligned} &2^{64} \times 4,096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} \\ &= 2^{76} \times 2^6 \text{ bytes} \\ &= 64 \text{ ZiB} \end{aligned}$$

Real-world les systèmes informatiques ne supportent rien de proche de ce maximum théorique. La taille du système de fichiers implémenté est actuellement limitée à 50 TiB pour ext4 et à 256 TiB pour NTFS.

Tailles des blocs de données

Le stockage de données sur un disque dur moderne est géré via l'adressage par blocs logiques, une couche d'abstraction qui permet au système d'exploitation de lire et d'écrire des données dans des

blocs logiques sans bien connaître le matériel sous-jacent. Le système d'exploitation s'appuie sur le périphérique de stockage pour mapper les blocs à ses secteurs physiques, et lit et écrit les données sur le disque à l'aide de blocs de données qui sont un multiple de la taille du secteur.

Amazon EBS annonce des secteurs physiques de 512 octets ou 4 096 octets (4 KiB) sur le système d'exploitation, en fonction des facteurs suivants :

1. Le type d'instance Amazon EC2
2. Système d'exploitation
3. La version du pilote NVMe

Amazon EBS annonce des secteurs physiques de 4 Ko uniquement si tous les facteurs le justifient. Si l'un d'entre eux ne prend pas en charge les secteurs physiques de 4 Ko, Amazon EBS annonce des secteurs physiques de 512 octets.

Prise en charge des types d'instances Amazon EC2

Le tableau suivant indique la taille des secteurs annoncés par Amazon EBS pour les différents types d'instances Amazon EC2.

Type d'instance	Linux	Windows
Tous les types d' Xen-based instances	Amazon EBS annonce toujours des secteurs physiques de 512 octets	
A1 C5 C5a C5ad C5d C5n C6g C6Gd DL1 3D D3en G4ad G4dn G5 G5G I3 I3en Inf1 M5 M5a M5ad M5d M5dn M5n M5Zn M6g M6Gg D P3dN P4D P4de R5 R5a R5ad R5d R5dn R5n R6g R6gd T3 T3a T4g X2Gd X2ieZn VT1 Z1d U-12tb1 U-18tb1 U-24tb1 U-3tb1 U-6tb1 U-9tb1	Amazon EBS annonce toujours des secteurs physiques de 512 octets	Amazon EBS annonce des secteurs physiques de 512 octets ou 4 Ko 1

Type d'instance	Linux	Windows
Toutes les autres Nitro-based instances	Amazon EBS annonce des secteurs physiques de 512 octets ou 4 Ko ¹	

¹ Cela dépend du support du système d'exploitation. Examinez la section suivante.

Support du système d'exploitation

Le tableau suivant fournit des exemples de systèmes d'exploitation et les tailles de secteurs physiques correspondantes annoncées par Amazon EBS. Cette liste n'est pas exhaustive. Nous vous recommandons de vérifier la taille du secteur physique annoncée par Amazon EBS dans votre système d'exploitation.

Système d'exploitation	Taille du secteur physique annoncé
<ul style="list-style-type: none"> Amazon Linux avec la version 4.14 du noyau et les versions antérieures RHEL 7.9 et versions antérieures Ubuntu 20.04 et versions antérieures Windows 7/Windows Server 2008 et versions antérieures 	512 octets
<ul style="list-style-type: none"> Amazon Linux avec noyau version 5.3 et versions ultérieures RHEL8.8 et plus tard Ubuntu 22.04 et versions ultérieures Windows 8/Windows Server 2012 et versions ultérieures ¹ 	4 Kio

¹ Pour les charges de travail Windows, assurez-vous d'utiliser la dernière version des pilotes [AWS NVMe](#). Amazon EBS annonce des secteurs physiques de 4 Ko avec les versions 1.4.1 et ultérieures du pilote AWS NVMe.

Non-default tailles des blocs

La taille par défaut du secteur pour les blocs de données logiques est actuellement de 4 Ko. Du fait que certaines charges de travail bénéficient d'une taille de taille inférieure ou supérieure, les systèmes de fichiers prennent en charge des tailles de blocs autres que par défaut et spécifiées au moment du formatage. Les scénarios dans lesquels des tailles de bloc autres que celles par défaut doivent être utilisées (optimisations, par exemple) sortent du cadre de cette rubrique, mais le choix de la taille de bloc a des conséquences sur la capacité de stockage du volume. Le tableau suivant montre la capacité de stockage théorique en fonction de la taille des blocs. Notez toutefois que la EBS-imposed limite de taille de volume (64 TiB pour io2 Block Express) est actuellement égale à la taille maximale autorisée par des blocs de données de 16 Ko.

Taille du bloc	Taille maximale du volume
4 Kio (par défaut)	16 TiO
8 Kio	32 Tio
16 Kio	64 Tio
32 Kio	128 Tio
64 Kio (maximum)	256 TiO

Volumes Amazon EBS et NVMe

Les volumes Amazon EBS sont exposés en tant que périphériques NVMe en mode bloc sur les instances Amazon EC2 basées sur le [AWS système Nitro](#). Pour tirer pleinement parti des performances et des fonctionnalités des volumes Amazon EBS exposés en tant que périphériques en mode bloc NVMe, le pilote AWS NVMe doit être installé sur l'instance EC2. Le pilote AWS NVMe est installé par défaut sur toutes les AMI AWS Windows et Linux de génération actuelle.

Si vous utilisez une AMI qui ne possède pas le pilote AWS NVMe, vous pouvez l'installer manuellement. Pour plus d'informations, consultez les pilotes [AWS NVMe](#) dans le guide de l'utilisateur Amazon EC2.

Instances Linux

Les noms des appareils sont `/dev/nvme0n1`, `/dev/nvme1n1`, et ainsi de suite. Les noms du périphérique que vous spécifiez dans un mappage de périphérique de stockage en mode bloc sont modifiés par les noms du périphérique NVMe (`/dev/nvme[0-26]n1`). Le pilote du périphérique de stockage en mode bloc peut attribuer les noms de périphériques NVMe dans un autre ordre que celui que vous avez spécifié pour les volumes dans le mappage de périphériques de stockage en mode bloc.

instances Windows

Lorsque vous associez un volume à votre instance, vous incluez un nom d'appareil pour le volume. Ce nom d'appareil est utilisé par Amazon EC2. Le pilote de périphérique en mode bloc de l'instance attribue le nom réel du volume lors du montage du volume, et le nom attribué peut être différent de celui utilisé par Amazon EC2.

Table des matières

- [Associer les volumes Amazon EBS aux noms des appareils NVMe](#)
- [Délai de I/O fonctionnement NVMe pour les volumes Amazon EBS](#)
- [NVMe Interruption commande pour les volumes Amazon EBS](#)

Associer les volumes Amazon EBS aux noms des appareils NVMe

EBS utilise la I/O virtualisation à racine unique (SR-IOV) pour fournir des pièces jointes aux volumes sur les Nitro-based instances utilisant la spécification NVMe. Ces périphériques dépendent des pilotes NVMe standard du système d'exploitation. Habituellement, ces pilotes détectent les périphériques attachés au démarrage de l'instance, puis créent des nœuds de périphériques selon l'ordre dans lequel les périphériques répondent, et non selon la spécification des périphériques dans le mappage de périphérique de stockage en mode bloc.

Instances Linux

<y>Sous Linux, les noms des périphériques NVMe suivent le modèle `/dev/nvme<x>n<y>`, où se <x> trouve l'ordre d'énumération, et, pour EBS, ils sont égaux à 1. Lors de démarrages consécutifs de l'instance, il arrive que les périphériques répondent à la détection dans un ordre différent, d'où un changement de nom des périphériques. En outre, le nom de périphérique attribué par le pilote de périphérique de stockage en mode bloc peut être différent du nom spécifié dans le mappage de périphérique de stockage en mode bloc.

Nous vous recommandons d'utiliser des identificateurs stables pour les volumes EBS au sein de votre instance, par exemple :

- Par Nitro-based exemple, les mappages de périphériques en mode bloc qui sont spécifiés dans la console Amazon EC2 lorsque vous connectez un volume EBS AttachVolume ou pendant des appels d'RunInstancesAPI sont capturés dans le champ de données spécifique au fournisseur de l'identification du contrôleur NVMe. Avec les AMI Amazon Linux ultérieures à la version 2017.09.01, nous fournissons une règle udev qui lit ces données et crée un lien symbolique vers le mappage de périphérique de stockage en mode bloc.
- L'ID de volume EBS et le point de montage sont stables entre les changements d'état d'instance. Le nom du périphérique NVMe peut changer en fonction de l'ordre dans lequel les périphériques répondent lors du démarrage de l'instance. Nous vous recommandons d'utiliser l'ID de volume EBS et le point de montage pour une identification cohérente des périphériques.
- Les volumes EBS NVMe ont l'ID de volume EBS comme numéro de série dans l'identification du périphérique. Utilisez la commande `lsblk -o +SERIAL` pour répertorier le numéro de série.
- Le format de nom de périphérique NVMe peut varier selon si le volume EBS a été attaché pendant ou après le lancement de l'instance. Les noms de périphériques NVMe pour les volumes attachés après le lancement de l'instance incluent le préfixe `/dev/`, tandis que les noms de périphériques NVMe pour les volumes attachés au cours du lancement de l'instance n'incluent pas le préfixe `/dev/`.
 - Pour Amazon Linux ou FreeBSD AMI, utilisez la commande `sudo ebsnvme-id /dev/nvme0n1 -u` pour obtenir un nom de périphérique NVMe cohérent.
 - Pour les autres distributions, utilisez la commande `sudo nvme id-ctrl -V /dev/nvme0n1` pour déterminer le nom du périphérique NVMe. Vous devrez peut-être inclure l'option `--vendor-specific` de commande.
- Lors du formatage d'un périphérique, un UUID est généré, qui persiste pendant toute la durée de vie du système de fichiers. Il est possible de spécifier une étiquette de périphérique au même moment. Pour plus d'informations, reportez-vous à [Mettre un volume Amazon EBS à disposition pour utilisation](#) la section [Démarrage à partir du mauvais volume](#).

AMI Amazon Linux

Avec l'AMI Amazon Linux 2017.09.01 ou ultérieure (y compris Amazon Linux 2), vous pouvez exécuter la commande `ebsnvme-id` comme suit afin de mapper le nom de périphérique NVMe à un ID de volume et un nom de périphérique :

L'exemple suivant illustre la commande et la sortie d'un volume attaché lors du lancement de l'instance. Notez que le nom du périphérique NVMe n'inclut pas le préfixe `/dev/`.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
Volume ID: vol-01324f611e2463981
sda
```

L'exemple suivant illustre la commande et la sortie d'un volume attaché après le lancement de l'instance. Notez que le nom du périphérique NVMe inclut le préfixe `/dev/`.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux crée également un lien symbolique entre le nom du périphérique du mappage de périphérique de stockage en mode bloc (par exemple, `/dev/sdf`) et le nom du périphérique NVMe.

AMI FreeBSD

À partir de FreeBSD 12.2-RELEASE, vous pouvez exécuter la commande `ebsnvme-id` comme indiqué ci-dessus. Transmettez le nom du périphérique NVMe (par exemple, `nvme0`) ou du périphérique de disque (par exemple, `nvd0` ou `nda0`). FreeBSD crée également des liens symboliques vers les périphériques de disque (par exemple, `/dev/aws/disk/ebs/volume_id`).

Autres AMI Linux

Avec la version 4.2 ou une version ultérieure du noyau, vous pouvez exécuter la commande `nvme id-ctrl` comme suit pour mapper un périphérique NVMe à un ID de volume. Commencez par installer le package de ligne de commande NVMe, `nvme-cli`, à l'aide des outils de gestion du package pour votre distribution Linux. Pour obtenir des instructions de téléchargement et d'installation pour d'autres distributions, reportez-vous à la documentation correspondante.

L'exemple suivant permet d'obtenir l'ID de volume et le nom de périphérique NVMe pour un volume attaché lors du lancement de l'instance. Notez que le nom du périphérique NVMe n'inclut pas le préfixe `/dev/`. Le nom de périphérique est disponible via une extension du contrôleur NVMe spécifique au fournisseur (octets 384:4095 de l'identification du contrôleur) :

```
[ec2-user ~]$ sudo nvme id-ctrl -V /dev/nvme0n1
NVME Identify Controller:
vid      : 0x1d0f
ssvid    : 0x1d0f
```

```
sn      : vol01234567890abcdef
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

L'exemple suivant permet d'obtenir l'ID de volume et le nom de périphérique NVMe pour un volume attaché après le lancement de l'instance. Notez que le nom du périphérique NVMe inclut le préfixe /dev/.

```
[ec2-user ~]$ sudo nvme id-ctrl -V /dev/nvme1n1
NVME Identify Controller:
vid      : 0x1d0f
ssvid    : 0x1d0f
sn       : volabcdef01234567890
mn       : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

La commande `lsblk` répertorie les périphériques disponibles ainsi que leurs points de montage (le cas échéant). Vous pouvez ainsi déterminer quel nom de périphérique utiliser. Dans cet exemple, /dev/nvme0n1p1 est monté comme périphérique racine et /dev/nvme1n1 est attaché mais pas monté.

```
[ec2-user ~]$ lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1             259:3   0  100G  0 disk
nvme0n1             259:0   0    8G  0 disk
  nvme0n1p1         259:1   0    8G  0 part /
  nvme0n1p128       259:2   0     1M  0 part
```

instances Windows

Vous pouvez exécuter la commande **ebsnvme-id** pour mapper le numéro de disque du périphérique NVMe à un ID de volume EBS et un nom de périphérique. Tous les périphériques NVMe EBS sont énumérés par défaut. Vous pouvez passer un numéro de disque pour énumérer des informations pour un périphérique spécifique. L'`ebsnvme-id` outil est inclus dans les dernières AMI Windows Server AWS fournies dans `C:\ProgramData\Amazon\Tools`.

À partir du package de pilotes AWS NVMe, 1.5.0, la dernière version de l'`ebsnvme-id` outil est installée par le package de pilotes. La dernière version n'est disponible que dans le package du pilote. Le lien de téléchargement autonome de l'outil `ebsnvme-id` ne recevra plus de mises à jour. La dernière version disponible via le lien autonome est 1.1.0, qui peut être téléchargée à l'aide du

lien [ebsnvme-id.zip](#) et ensuite extraire le contenu vers votre instance Amazon EC2 pour accéder à `ebsnvme-id.exe`.

```
PS C:\ProgramData\Amazon\Tools> ebsnvme-id.exe
```

```
Disk Number: 0
```

```
Volume ID: vol-0d6d7ee9f6e471a7f
```

```
Device Name: sda1
```

```
Disk Number: 1
```

```
Volume ID: vol-03a26248ff39b57cf
```

```
Device Name: xvdd
```

```
Disk Number: 2
```

```
Volume ID: vol-038bd1c629aa125e6
```

```
Device Name: xvde
```

```
Disk Number: 3
```

```
Volume ID: vol-034f9d29ec0b64c89
```

```
Device Name: xvdb
```

```
Disk Number: 4
```

```
Volume ID: vol-03e2dbe464b66f0a1
```

```
Device Name: xvdc
```

```
PS C:\ProgramData\Amazon\Tools> ebsnvme-id.exe 4
```

```
Disk Number: 4
```

```
Volume ID: vol-03e2dbe464b66f0a1
```

```
Device Name: xvdc
```

Délai de I/O fonctionnement NVMe pour les volumes Amazon EBS

La plupart des systèmes d'exploitation spécifient un délai d'attente pour les I/O opérations soumises aux périphériques NVMe.

Instances Linux

Sous Linux, les volumes EBS attachés aux Nitro-based instances utilisent le pilote NVMe par défaut fourni par le système d'exploitation. La plupart des systèmes d'exploitation spécifient un délai d'attente pour les I/O opérations soumises aux périphériques NVMe. Le délai d'attente par défaut est de 30 secondes. Il peut être modifié à l'aide du paramètre de démarrage `nvme_core.io_timeout`. Pour la plupart des noyaux Linux antérieurs à la version 4.6, ce paramètre est `nvme.io_timeout`.

Si la I/O latence dépasse la valeur de ce paramètre de délai d'attente, le pilote Linux NVMe échoue I/O et renvoie une erreur au système de fichiers ou à l'application. En fonction de l' I/O opération, votre système de fichiers ou votre application peut réessayer de corriger l'erreur. Dans certains cas, il est possible de remonter le système de fichiers en lecture seule.

Pour bénéficier d'une expérience similaire à celles des volumes EBS attachés aux instances Xen, nous vous recommandons de définir `nvme_core.io_timeout` sur la valeur la plus élevée possible. Pour les noyaux actuels, le maximum est 4294967295, alors que pour les noyaux précédents, le maximum est 255. Selon la version de Linux, il se peut que la temporisation soit déjà réglée à la valeur maximale prise en charge. Par exemple, la temporisation est réglée sur 4294967295 par défaut pour les AMI Linux Amazon 2017.09.01 et ultérieures.

Vous pouvez vérifier la valeur maximale pour votre distribution de Linux en écrivant une valeur plus élevée que la valeur maximale suggérée dans `/sys/module/nvme_core/parameters/io_timeout` et en recherchant l'erreur `Numerical result out of range` au moment d'enregistrer le fichier.

instances Windows

Sous Windows, le délai d'expiration par défaut est de 60 secondes et le maximum est de 255 secondes. Vous pouvez modifier le paramètre de registre de classe de disque `TimeoutValue` à l'aide de la procédure décrite sur la page [Registry Entries for SCSI Miniport Drivers](#).

NVMe Interruption commande pour les volumes Amazon EBS

La `Abort` commande est une commande d'administration NVMe qui est émise pour mettre fin à une commande spécifique précédemment soumise au contrôleur. Cette commande est généralement envoyée par le pilote de périphérique aux périphériques de stockage qui ont dépassé le seuil de temporisation de I/O fonctionnement.

Les types d'instances Amazon EC2 qui prennent en charge la `Abort` commande par défaut mettront fin à une commande spécifique qui a été précédemment soumise au contrôleur lorsqu'une `Abort` commande est émise pour des volumes Amazon EBS attachés. Les instances Amazon EC2 qui ne prennent pas en charge la `Abort` commande n'entreprennent aucune action lorsqu'une `Abort` commande est émise pour des volumes Amazon EBS attachés.

La `Abort` commande est prise en charge par :

- Appareils Amazon EBS dotés d'un appareil NVMe version 1.4 ou supérieure.

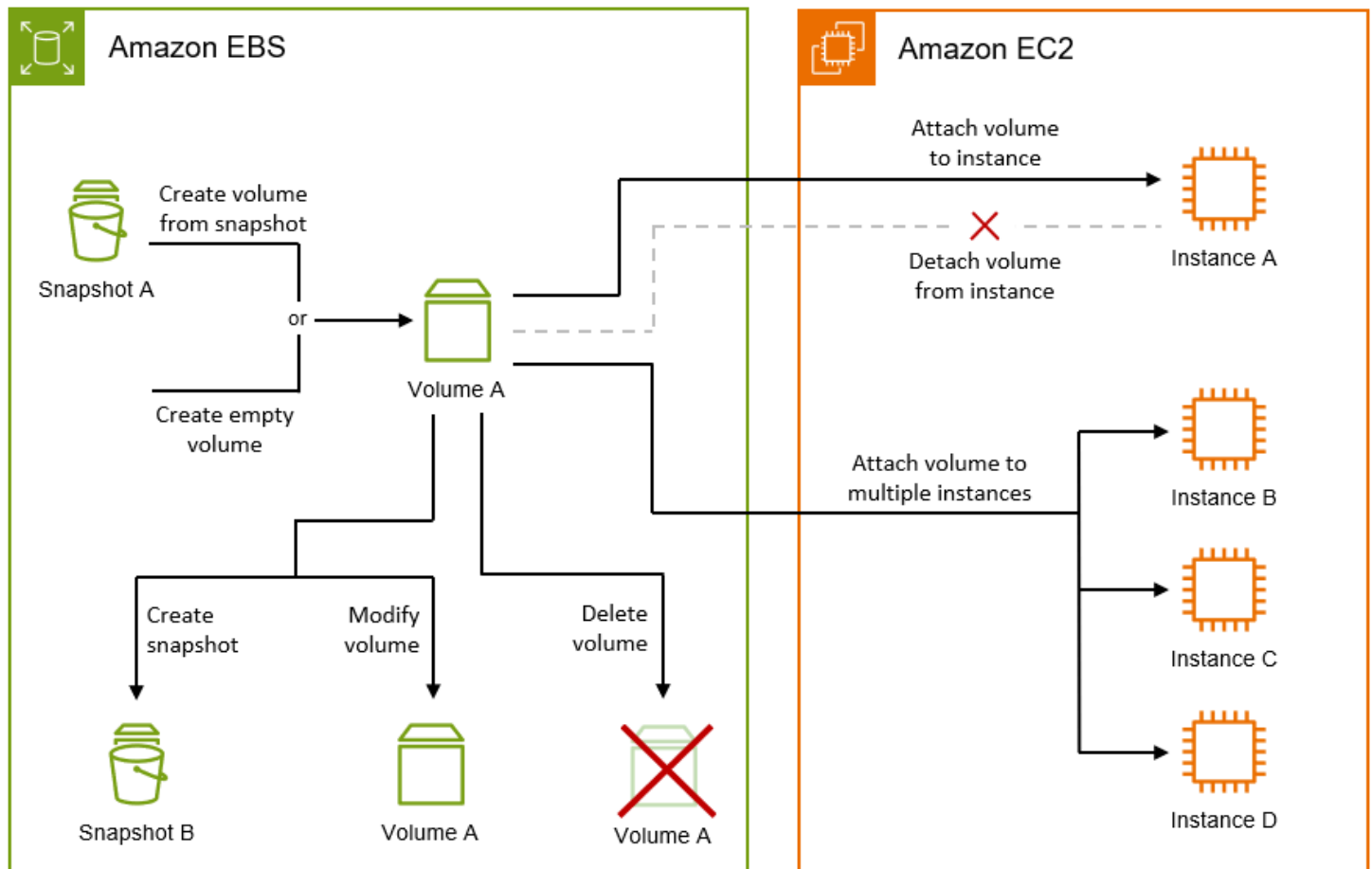
- Toutes les instances Amazon EC2, à l'exception Xen-based des types d'instances et des types d'Nitro-based instances suivants :
 - Usage général : A1 | M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6g | M6gd | Mac1 | Mac2 | T3 | T3a | T4g
 - Optimisation du calcul : C5 | c5a | C5ad | C5d | C5n | C6g | C6gd
 - Mémoire optimisée : R5 | R5a | R5ad | R5d | R5dn | R5n | R6g | R6gd | | | | | X2GD | X2ieZn | Z1d U-12tb1 U-18tb1 U-24tb1 U-3tb1 U-6tb1 U-9tb1
 - Optimisées en stockage : D3 | D3en | I3en
 - Calcul accéléré : DL1 | G4ad | G4dn | G5 | G5g | Inf1 | P3dn | P4d | P4de | VT1

Pour plus d'informations, reportez-vous à la section [Abort 5.1](#) de la spécification [de base](#) NVM Express.

Cycle de vie des volumes Amazon EBS

Le cycle de vie d'un volume Amazon EBS commence par le processus de création. Vous pouvez créer un volume à partir d'un instantané Amazon EBS ou créer un volume vide. Avant de pouvoir utiliser votre volume, vous devez l'associer à une ou plusieurs instances Amazon EC2 situées dans la même zone de disponibilité que le volume. Vous pouvez associer plusieurs volumes à une instance. Si nécessaire, vous pouvez détacher un volume d'une instance, puis l'associer à une autre instance. Si vos besoins en stockage changent, vous pouvez modifier la taille ou les performances du volume à tout moment. Vous pouvez créer des sauvegardes ponctuelles de vos volumes en créant des instantanés Amazon EBS. Si vous n'avez plus besoin d'un volume, vous pouvez le supprimer pour ne plus encourir les coûts de stockage associés.

L'image suivante montre les actions que vous pouvez effectuer sur vos volumes dans le cadre de leur cycle de vie. Vous pouvez également effectuer certaines tâches en vous connectant à l'instance et en exécutant une commande du système d'exploitation. Par exemple, le formatage du volume, le montage du volume, la gestion des partitions et l'affichage de l'espace disque disponible.



Tâches

- [Créez un volume Amazon EBS.](#)
- [Partager un volume](#)
- [Copier un volume Amazon EBS](#)
- [Attacher un volume Amazon EBS à une instance Amazon EC2](#)
- [Attachez un volume EBS à plusieurs instances EC2 à l'aide de Multi-Attach](#)
- [Mettre un volume Amazon EBS à disposition pour utilisation](#)
- [Afficher des informations sur un volume Amazon EBS](#)
- [Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes](#)
- [Détacher un volume Amazon EBS d'une instance Amazon EC2](#)
- [Supprimer un volume Amazon EBS](#)

Créez un volume Amazon EBS.

Vous pouvez créer un volume Amazon EBS, puis l'attacher à n'importe quelle instance EC2 dans la même zone de disponibilité.

Vous pouvez soit créer un volume vide, soit créer un volume à partir d'un instantané Amazon EBS. Si vous créez un volume à partir d'un instantané, le volume commence comme une réplique exacte du volume qui a été utilisé pour créer cet instantané.

Initialisation du volume

Lorsque vous créez un volume à partir d'un instantané, les blocs de stockage de l'instantané doivent être téléchargés depuis Amazon S3 et écrits sur le volume pour que vous puissiez y accéder. Ce processus est appelé initialisation du volume. Pendant ce temps, le volume connaîtra une I/O latence accrue. Les performances complètes du volume ne sont atteintes qu'une fois que tous les blocs de stockage ont été téléchargés et écrits sur le volume.

Le taux d'initialisation du volume par défaut fluctue tout au long du processus d'initialisation, ce qui peut rendre les délais d'exécution imprévisibles.

Pour minimiser les impacts sur les performances associés à l'initialisation des volumes, vous pouvez utiliser un taux provisionné Amazon EBS pour l'initialisation des volumes (taux d'initialisation des volumes) ou une restauration rapide des instantanés. Pour plus d'informations, consultez [Initialiser les volumes Amazon EBS](#).

Chiffrement de volume

L'état de chiffrement du volume dépend de l'[activation du chiffrement par défaut](#) sur votre compte et de l'état de chiffrement de l'instantané, si vous choisissez d'en utiliser un. Le tableau suivant récapitule les résultats de chiffrement possibles.

Chiffrement par défaut	Snapshot utilisé ?	Résultat du chiffrement des volumes	Remarque
Désactivé	Non	Chiffrement en option	Si vous activez le chiffrement, vous pouvez spécifier la clé KMS à utiliser. Si vous activez le chiffrement mais que vous ne spécifiez pas de clé KMS, la Clé gérée par AWS (aws/ebs) est utilisée.

Chiffrement par défaut	Snapshot utilisé ?	Résultat du chiffrement des volumes	Remarque
Désactivé	Oui, non chiffré	Chiffrement en option	Si vous activez le chiffrement, vous pouvez spécifier la clé KMS à utiliser. Si vous activez le chiffrement mais que vous ne spécifiez pas de clé KMS, la Clé gérée par AWS (aws/ebs) est utilisée.
Désactivé	Oui, crypté	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, le volume est chiffré à l'aide de la même clé KMS que le snapshot source.
Activé	Non	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.
Activé	Oui, non chiffré	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.
Activé	Oui, crypté	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, le volume est chiffré à l'aide de la même clé que le snapshot source (console) ou de la clé spécifiée pour le chiffrement par défaut (CLI/API).

Considérations supplémentaires

- Les volumes doivent être attachés à des instances situées dans la même zone de disponibilité.
- Les volumes ne sont prêts à être utilisés qu'après leur entrée dans l'état `available`.

- Lorsque vous créez un volume à l'aide de la console, gp3 c'est le type de volume par défaut. Pour les outils de ligne de commande, l'API et le SDK, gp2 c'est le type de volume par défaut.
- Pour utiliser un volume avec une instance exécutée sur un avant-poste, vous devez créer le volume sur le même avant-poste que l'instance.
- Si vous créez un volume à utiliser avec une instance Windows et que sa taille est supérieure à 2 048 Gio, assurez-vous de configurer le volume pour utiliser des tables de partitions GPT. Pour plus d'informations, consultez [Contraintes de volume Amazon EBS](#) la section Support [Windows pour les disques de plus de 2 To.](#)
- Les volumes sont également créés indirectement en lançant une instance Amazon EC2. Soit l'AMI utilisée pour lancer l'instance, soit la demande de lancement de l'instance elle-même peut inclure des mappages de périphériques en mode bloc pour les volumes Amazon EBS. Pour plus d'informations, voir [Bloquer les mappages](#) d'appareils.

Console

Pour créer un de volumes

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Volumes, puis sélectionnez Créer un volume.
3. (Outpostclients uniquement) Pour Outpost ARN, entrez l'ARN du volume AWS Outpost sur lequel vous souhaitez créer le volume.
4. Pour Volume type (Type de volume), choisissez le type de volume à créer. Pour plus d'informations sur les types de volumes disponibles, consultez [Types de volume Amazon EBS](#).
5. Pour Size (Taille), saisissez la taille du volume en Gio. Pour plus d'informations, consultez [Contraintes de volume Amazon EBS](#).
6. (Pour *io1io2*, et *gp3* uniquement) Pour les IOPS, entrez le nombre maximum d' input/output opérations par seconde (IOPS) que le volume doit fournir.
7. (Pour *gp3* uniquement) Pour le débit, entrez le débit que le volume doit fournir, dans MiB/s.
8. Pour Zone de disponibilité, choisissez la zone de disponibilité dans laquelle créer le volume.
9. Pour Snapshot ID, effectuez l'une des opérations suivantes :
 - Pour créer un volume vide, conservez la valeur par défaut (Ne créez pas de volume à partir d'un instantané).
 - Pour créer le volume à partir d'un instantané, sélectionnez le cliché à utiliser.

10. Si vous avez sélectionné un instantané, pour Taux d'initialisation du volume, vous pouvez éventuellement spécifier le taux d'initialisation du volume, dans MiB/s, auquel les blocs de clichés doivent être téléchargés depuis Amazon S3 vers le volume après leur création. Pour plus d'informations, consultez [Utiliser un tarif provisionné par Amazon EBS pour l'initialisation des volumes](#). Pour utiliser le taux d'initialisation par défaut ou la restauration rapide des instantanés (si elle est activée pour l'instantané sélectionné), ne spécifiez pas de taux.
11. (*io1* et *io2* uniquement) Pour activer le volume pour Amazon EBS Multi-Attach, sélectionnez Activer Multi-Attach. Pour plus d'informations, consultez [Attachez un volume EBS à plusieurs instances EC2 à l'aide de Multi-Attach](#).
12. Définissez l'état du chiffrement du volume.
 - Si le [cryptage de votre compte est activé par défaut](#), le cryptage est automatique et ne peut pas être désactivé.
 - Si vous avez sélectionné un instantané chiffré, le chiffrement est automatique et ne peut pas être désactivé.
 - Si le [chiffrement de votre compte n'est pas activé par défaut](#) et que vous sélectionnez un instantané non chiffré ou que vous ne sélectionnez aucun instantané, le cryptage est facultatif.
13. (Facultatif) Pour attribuer des balises personnalisées au volume, dans la section Balises, choisissez Ajouter une balise, puis entrez une paire clé-valeur de balise.
14. Choisissez Créer un volume.
15. Pour utiliser le volume, attendez qu'il atteigne `available` cet état, puis attachez-le à une instance Amazon EC2 dans la même zone de disponibilité. Pour plus d'informations, consultez [Attacher un volume Amazon EBS à une instance Amazon EC2](#).

AWS CLI

Pour créer un de volumes

Utilisez la commande [create-volume](#). L'exemple suivant crée un volume `gp3` vide d'une taille de 100 GiB dans la zone de disponibilité spécifiée.

```
aws ec2 create-volume \  
  --volume-type gp3 \  
  --size 100 \  
  --availability-zone us-east-1a
```

PowerShell

Pour créer un de volumes

Utilisez l'applet de commande [New-EC2Volume](#). L'exemple suivant crée un volume gp3 vide d'une taille de 100 GiB dans la zone de disponibilité spécifiée.

```
New-EC2Volume `
  -VolumeType gp3 `
  -Size 100 `
  -AvailabilityZone us-east-1a
```

Partager un volume

Vous pouvez utiliser AWS Resource Access Manager (AWS RAM) pour partager des volumes Amazon EBS avec d'autres AWS comptes. Après avoir partagé un volume, les comptes utilisateurs peuvent consulter les informations relatives au volume et créer des copies du volume partagé dans la même zone de disponibilité. Pour plus d'informations sur la création de copies, consultez [Copier un volume Amazon EBS](#). Les comptes utilisateurs ne peuvent pas joindre, modifier, supprimer ou créer des instantanés d'un volume partagé.

Par exemple, vous pouvez partager des volumes de production avec des comptes de développement pour actualiser les environnements de test avec des données de production à jour tout en préservant l'isolation au niveau du compte.

Vous pouvez partager des volumes qui sont les suivants :

- Non chiffré
- Chiffré avec une clé gérée par le client

Vous ne pouvez pas partager des volumes chiffrés avec la clé AWS gérée par défaut pour Amazon EBS.

Table des matières

- [Permissions](#)
- [Partager un volume](#)
- [Afficher les volumes partagés](#)

- [Considérations relatives au partage de volumes](#)
- [Surveillez l'activité de partage](#)
- [Volumes partagés et corbeille](#)
- [Tarification](#)

Permissions

Lorsque vous créez un partage de ressources pour des volumes partagés, vous devez associer des autorisations gérées au partage de ressources. Les autorisations gérées déterminent les actions que les comptes consommateurs peuvent effectuer sur les volumes partagés du partage de ressources. AWS RAM fournit les autorisations AWS gérées suivantes :

- `AWSRAMDefaultPermissionEBSVolume`(par défaut) — Autorise les comptes consommateurs à consulter les informations relatives aux volumes.
- `AWSRAMPermissionEBSVolumeCopyAccess`— Autorise les comptes utilisateurs à consulter les informations relatives au volume et à créer des copies du volume partagé.

Vous pouvez également créer une autorisation gérée par le client pour le type de `ec2:Volume` ressource. Pour plus d'informations, consultez la section [Création et utilisation des autorisations gérées par le client](#) dans le Guide de AWS RAM l'utilisateur.

Partager un volume

Utilisez l'une des méthodes suivantes pour partager un volume Amazon EBS.

Console

Pour partager un volume

1. Ouvrez la console Amazon Elastic Compute Cloud à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume, puis choisissez Actions, Partager le volume.
4. Effectuez l'une des actions suivantes :
 - Pour ajouter le volume à un partage de ressources existant, sélectionnez le partage de ressources.

- Pour créer un nouveau partage de ressources, choisissez **Créer un nouveau partage de ressources**. Cela ouvre la AWS RAM console, dans laquelle vous configurez le partage.
5. Pour les directeurs, ajoutez les comptes avec lesquels partager le volume. Vous pouvez ajouter des identifiants de compte individuels, des unités organisationnelles (UO) ou l'ensemble de votre organisation.
 6. Pour les autorisations gérées, choisissez l'une des options suivantes :
 - **AWSRAMDefaultPermissionEBSVolume**(par défaut) — Les comptes consommateurs peuvent uniquement afficher les métadonnées des volumes.
 - **AWSRAMPermissionEBSVolumeCopyAccess**— Les comptes utilisateurs peuvent consulter les métadonnées du volume et créer des copies du volume partagé.
 - Autorisation gérée par le client que vous avez créée pour le type de `ec2:Volume` ressource.
 7. Choisissez **Créer une ressource**.

AWS CLI

Utilisez la commande [create-resource-share](#). Spécifiez l'ARN du volume, le compte consommateur et l'ARN d'autorisation. Pour trouver l'ARN du volume, appelez <https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-volumes.html> `describe-volumes`. La réponse inclut le `VolumeArn` champ correspondant à chaque volume.

L'exemple suivant crée un partage de ressources qui partage le volume `vol-1234567890abcdef0` avec `222222222222` le compte et attribue l'autorisation `AWSRAMPermissionEBSVolumeCopyAccess` gérée :

```
aws ram create-resource-share \
--name my-volume-share \
--resource-arns arn:aws:ec2:us-east-1:111111111111:volume/vol-1234567890abcdef0 \
--principals 222222222222 \
--permission-arns arn:aws:ram::aws:permission/AWSRAMPermissionEBSVolumeCopyAccess \
--region us-east-1
```

Pour partager avec l'autorisation par défaut (`AWSRAMDefaultPermissionEBSVolumeDescription` uniquement), omettez le `--permission-arns` paramètre :

```
aws ram create-resource-share \
```



```
--name my-volume-share \  
--resource-arns arn:aws:ec2:us-east-1:111111111111:volume/vol-1234567890abcdef0 \  
--principals 222222222222 \  
--region us-east-1
```

Pour plus d'informations sur les partages de ressources, consultez [la section Création d'un partage de ressources](#) dans le Guide de AWS RAM l'utilisateur.

Afficher les volumes partagés

Une fois que vous avez créé le partage de ressources, les comptes spécifiés reçoivent une invitation. Les comptes extérieurs à votre organisation AWS Organizations doivent accepter l'invitation pour pouvoir accéder aux volumes partagés. Pour plus d'informations, voir [Accepter et rejeter les invitations à partager des ressources](#) dans le Guide de l'AWS RAM utilisateur.

Vous pouvez consulter les volumes partagés avec votre compte à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les volumes partagés

1. Ouvrez la console Amazon Elastic Compute Cloud à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Effectuez l'une des actions suivantes :
 - Choisissez le filtre prédéfini Partagé avec moi pour afficher tous les volumes partagés avec votre compte.
 - Choisissez Ajouter un filtre, ID du propriétaire, puis saisissez l'ID du compte de partage.

Les volumes partagés affichent l'ID du compte de partage dans la colonne ID du propriétaire.

AWS CLI

Utilisez la [commande](#) `describe-volumes` avec le `owner-id` filtre pour afficher les volumes partagés avec vous par un compte spécifique.

```
aws ec2 describe-volumes \  

```

```
--filters Name=owner-id,Values=111111111111 \  
--region us-east-1
```

Les volumes partagés incluent le OwnerId champ de la réponse, qui indique l'ID du compte de partage.

Considérations relatives au partage de volumes

Lorsque vous partagez des volumes avec d'autres comptes, tenez compte des points suivants.

- Vous pouvez partager des volumes non chiffrés et des volumes chiffrés à l'aide d'une clé gérée par le client. Vous ne pouvez pas partager des volumes chiffrés avec la clé AWS gérée par défaut pour Amazon EBS.
- Pour partager un volume, le compte du propriétaire du volume doit être `kms:DescribeKey` autorisé à utiliser la clé de chiffrement Amazon EBS par défaut. Cela est obligatoire pour tous les volumes, y compris les volumes non chiffrés, car le service valide l'état de chiffrement du volume pendant le processus de partage.
- Pour partager un volume chiffré avec une clé gérée par le client, vous devez également partager la clé KMS avec le compte utilisateur. Pour plus d'informations, consultez [Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS](#) dans le Guide du développeur AWS Key Management Service .
- Pour créer des copies d'un volume chiffré partagé, le compte utilisateur a besoin de `kms:CreateGrant`, `kms:GenerateDataKey`, `kms:GenerateDataKeyWithoutPlaintext`, `kms:ReEncrypt*`, et `kms:Decrypt` sur la clé KMS.
- Les comptes utilisateurs ne peuvent pas joindre, modifier, supprimer ou créer des instantanés d'un volume partagé. Ils peuvent uniquement consulter les métadonnées des volumes et en créer des copies.
- Une seule opération de copie peut être en cours sur un volume partagé à la fois, pour tous les comptes avec lesquels le volume est partagé. Les demandes de copie supplémentaires renvoient une erreur jusqu'à ce que l'opération en cours soit terminée.
- Les noms des zones de disponibilité (tels que `us-east-1a`) correspondent à différents emplacements physiques dans différents AWS comptes. Utilisez les identifiants de zone de disponibilité (tels que `us-east-1-az1`) pour identifier le même emplacement physique sur tous les comptes. Pour plus d'informations, consultez [la section ID de zone de disponibilité pour vos AWS ressources](#) dans le Guide de l'utilisateur AWS IAM.

- La suppression d'un volume d'un partage de ressources n'annule pas les opérations de copie en cours.
- La suppression du volume source n'annule pas les opérations de copie en cours.

Surveillez l'activité de partage

AWS CloudTrail Journalisation de l'API

Tous les appels d'API de partage de volumes et de copie sont enregistrés AWS CloudTrail.

CopyVolumes Les appels d'API sont enregistrés à la fois pour le compte qui initie la copie et pour le compte du propriétaire du volume. Pour plus d'informations, consultez la section [Journalisation des appels d'API Amazon Elastic Compute Cloud avec AWS CloudTrail](#).

EventBridge Notifications Amazon

Amazon EBS envoie des EventBridge événements Amazon lorsque les opérations de copie entre comptes sont terminées. Le propriétaire du volume et le compte consommateur reçoivent tous deux l'événement. Les événements de copie de volume utilisent le type de détail EBS `Volume Notification` avec le nom de l'événement `sharedVolumeCopy`. L'événement inclut l'ID du volume, l'état d'achèvement (`completed` ou `failed`) et un horodatage.

Pour configurer les notifications, créez une EventBridge règle Amazon qui associe les EBS `Volume Notification` événements au nom de l'`sharedVolumeCopy` événement. Pour plus d'informations, consultez la section EventBridge Événements [Amazon pour Amazon EBS](#).

Volumes partagés et corbeille

Si vous avez une règle de conservation de la corbeille qui s'applique aux volumes, la suppression d'un volume partagé le déplace vers la Corbeille. Le volume reste dans ses parts de AWS RAM ressources tout au long de la période de conservation. Lorsque vous restaurez le volume depuis la corbeille, il est accessible via les mêmes partages de ressources auxquels il appartenait avant la suppression.

Notez le comportement de partage de ressources suivant pour un volume qui se trouve dans la corbeille :

- Si vous avez supprimé un compte du partage de ressources alors que le volume se trouvait dans la corbeille, la restauration du volume n'autorise pas à nouveau l'accès à ce compte.

- Si vous avez ajouté un compte au partage de ressources alors que le volume était dans la corbeille, ce compte a accès au volume après la restauration.

Après avoir restauré un volume depuis la corbeille, vérifiez que seuls les comptes prévus y ont accès en consultant vos partages de ressources dans la [AWS RAM console](#).

Tarification

Le partage des volumes est gratuit AWS RAM. Le compte qui crée une copie paie les frais de copie en volume et les frais de volume Amazon EBS habituels pour le nouveau volume. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Copier un volume Amazon EBS

Une copie de volume est une copie instantanée et cohérente du volume source. Il inclut tous les blocs de données écrits sur le volume source au moment où l'initialisation de la copie du volume commence. La copie du volume reçoit son propre identifiant de volume unique. Les copies de volume sont créées immédiatement et peuvent être attachées à une instance Amazon EC2 une fois que celle-ci atteint `available` cet état. Grâce aux copies en volume, vous pouvez rapidement copier vos données de production pour les environnements de test et de développement.

Vous pouvez également créer des copies à partir de volumes partagés avec vous par d'autres AWS comptes. Pour copier un volume depuis un autre compte, le volume source doit être partagé avec vous via AWS Resource Access Manager (AWS RAM). Pour plus d'informations, consultez [Partager un volume](#).

Initialisation

Les copies de volume sont initialisées après leur création. Lors de l'initialisation, les blocs de données sont copiés depuis le volume source et écrits sur la copie du volume en arrière-plan. Le volume reste dans `initializing` cet état jusqu'à la fin de l'initialisation.

Performances lors de l'initialisation

Les opérations de copie n'ont aucune incidence sur les performances du volume source. Vous pouvez continuer à utiliser le volume source normalement pendant le processus de copie. Les volumes copiés sont accessibles instantanément sans attendre que les données soient copiées depuis le volume source. Les copies en volume fournissent un accès instantané aux données avec

une latence d'un chiffre en millisecondes. Cependant, la latence réelle peut varier en fonction du type de volume. Lors de l'initialisation, la copie du volume fournit des performances de base égales à la plus faible des trois valeurs suivantes :

- 3 000 input/output opérations par seconde (IOPS) et 125 MiB/s
- Les performances provisionnées pour le volume source
- Les performances provisionnées pour la copie du volume

La copie du volume peut dépasser les performances de base lorsque les critères suivants sont remplis :

1. Le volume source et la copie du volume sont provisionnés avec plus de 3 000 IOPS et 125 IOPS. MiB/s
2. Le volume source possède une capacité de performance inutilisée (les performances pilotées sont inférieures aux performances provisionnées).

Par exemple, si le volume source est provisionné avec 10 000 IOPS et que votre charge de travail ne génère actuellement que 5 000 IOPS, et que la copie du volume est provisionnée avec 10 000 IOPS, la copie du volume peut atteindre des performances supérieures aux performances de référence de 3 000 IOPS par seconde lors de l'initialisation en utilisant les 5 000 IOPS inutilisées du volume source.

Durée d'initialisation

Le temps nécessaire pour initialiser une copie de volume dépend de la taille des données de bloc écrites sur le volume source au moment de la création de la copie de volume. Les copies de volume sont initialisées dans la mesure du possible, selon les directives générales suivantes. Pour les 1 premiers TiB de blocs de données, l'initialisation du volume prend jusqu'à 6 heures. Pour chaque TiB suivant de blocs de données jusqu'à 16 TiB, l'initialisation prend 1,2 heure par TiB. Pour les données écrites supérieures à 16 TiB, l'initialisation prend 24 heures.

Surveiller la progression de l'initialisation

Vous pouvez suivre la progression de l'initialisation à l'aide de la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-volume-status.html> AWS CLI describe-volume-status ou d'Amazon. EventBridge Pour plus d'informations, consultez [Surveiller l'état de l'initialisation](#) du volume Amazon EBS.

Chiffrement

Lorsque vous copiez un volume, le chiffrement de la copie dépend de l'état de chiffrement du volume source, du paramètre de chiffrement par défaut de votre compte et des `KmsKeyId` paramètres `Encrypted` et que vous spécifiez dans la demande de copie.

Volumes sources non chiffrés

Si le volume source n'est pas chiffré et que le chiffrement par défaut est désactivé pour votre compte, la copie n'est pas chiffrée. Vous pouvez chiffrer la copie en réglant le `Encrypted` paramètre sur `true`. Si vous ne spécifiez pas de KMS key, la clé de chiffrement Amazon EBS par défaut de votre compte est utilisée.

Si le volume source n'est pas chiffré et que le chiffrement est activé par défaut pour votre compte, la copie est automatiquement cryptée. Si vous ne spécifiez pas de KMS key, la clé de chiffrement Amazon EBS par défaut de votre compte est utilisée.

Volumes sources chiffrés

Si le volume source est chiffré, la copie est toujours chiffrée. Vous ne pouvez pas créer de copie non chiffrée à partir d'un volume source chiffré.

Pour les copies du même compte, la copie utilise la même clé KMS que le volume source par défaut. Vous pouvez spécifier une autre clé gérée par le client pour rechiffrer la copie.

Pour les copies entre comptes, la copie utilise la clé de cryptage Amazon EBS par défaut de votre compte. Vous pouvez spécifier une autre clé gérée par le client dans le `KmsKeyId` paramètre. Vous pouvez utiliser la clé KMS du compte source pour chiffrer la copie du volume si cette clé a été partagée avec votre compte.

Cross-account exigences en matière de chiffrement

Pour copier un volume partagé chiffré à l'aide d'une clé gérée par le client, le propriétaire du volume doit partager la clé KMS avec votre compte. Pour plus d'informations, consultez la section [Autoriser les utilisateurs d'autres comptes à utiliser un KMS key](#) dans le Guide du AWS Key Management Service développeur.

Les volumes chiffrés avec la clé AWS gérée par défaut pour Amazon EBS ne peuvent pas être partagés ou copiés entre les comptes.

Résultats du chiffrement

Volumes sources non chiffrés

Chiffrement par défaut	Vous spécifiez un KMS key	Résultat
Désactivé	Non	La copie n'est pas chiffrée
Désactivé	Oui	Copie chiffrée avec la clé spécifiée
Activé	Non	Copie chiffrée avec la clé de chiffrement Amazon EBS par défaut de votre compte
Enabled	Oui	Copie chiffrée avec la clé spécifiée

Volumes sources chiffrés (même compte)

Vous spécifiez un KMS key	Résultat
Non	Copie chiffrée avec la même clé que le volume source
Oui	Copie rechiffrée avec la clé spécifiée

Volumes sources chiffrés (entre comptes)

Vous spécifiez un KMS key	Résultat
Non	Copie chiffrée avec la clé de chiffrement Amazon EBS par défaut de votre compte
Oui	Copie chiffrée avec la clé spécifiée

Cross-account les copies ne réutilisent jamais la clé KMS du compte source par défaut. Si vous souhaitez utiliser une clé du compte source, celle-ci doit être partagée avec votre compte.

Considérations

- Une copie de volume capture un état ponctuel et constant du volume source en cas de panne. Il inclut uniquement les données qui ont été écrites dans le volume au moment de la demande de copie. Il n'inclut pas les données mises en cache par les applications ou le système d'exploitation. Pour obtenir des copies cohérentes avec les applications, interrompez les écritures sur le volume ou mettez l'application au repos avant de créer la copie. Pour les bases de données, utilisez le mécanisme approprié pour vider les pages sales et les bloquer I/O (par exemple `fsfreeze` sous Linux ou VSS sous Windows). Vous pouvez reprendre les écritures une fois la demande de copie renvoyée.
- Vous ne pouvez créer qu'une seule copie de volume à partir d'un volume source à la fois. Vous ne pouvez créer des copies suivantes du même volume source qu'une fois que la copie du volume précédent a été complètement initialisée.
- Vous pouvez avoir un maximum de 5 copies de volume en cours par région. Si vous dépassez ce quota, le `CopyVolumesLimitExceeded` message d'erreur s'affiche. Vous pouvez [demander une augmentation de quota](#) si nécessaire.
- La copie du volume doit être créée dans la même zone de disponibilité que le volume source.
- La taille de la copie du volume doit être égale ou supérieure à la taille du volume source.
- Vous ne pouvez pas copier une copie de volume pendant sa création ou son initialisation.
- Pour créer une copie de volume, le volume source doit être à l'`in-use` état `available` ou et les modifications de volume doivent être à l'`optimizing` état `completed` ou.
- Les copies en volume sont soumises aux mêmes quotas de compte et de stockage régional et d'IOPS que les volumes Amazon EBS classiques. Pour en savoir plus, consultez la section [Quotas Amazon EBS](#).
- Si vous supprimez le volume source alors que l'opération de copie est en cours, celle-ci est toujours terminée.
- Les balises attribuées au volume source ne sont pas attribuées à la copie du volume.
- Vous ne pouvez pas créer de copies à partir de volumes situés sur Outposts ou dans Wavelength Zones.

Tarification

Lorsque vous créez une copie d'un volume source, l'opération de copie vous est facturée. Les frais d'opération de copie sont basés sur la taille des blocs de données écrits sur le volume source au moment de la création de la copie. Le volume nouvellement créé est facturé de la même manière que

tout autre volume Amazon EBS. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Copier un volume

Utilisez l'une des méthodes suivantes pour copier un volume Amazon EBS.

Console

Pour copier un volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume à copier et choisissez Actions, Copier le volume.
4. Dans Type de volume, choisissez le type de volume pour la copie. Le type de volume par défaut est gp3.
5. Dans Taille, entrez la taille de la copie du volume, dans GiBs. La taille doit être égale ou supérieure à la taille du volume source.
6. (*io1* et *io2*, et *gp3* uniquement) Pour les IOPS, entrez le nombre maximum d' input/output opérations par seconde (IOPS) pour la copie du volume.
7. (*gp3* uniquement) Pour Débit, entrez le débit de la copie du volume, dans MiB/s.
8. (*io1* et *io2* uniquement) Pour activer la copie de volume pour Amazon EBS Multi-Attach, sélectionnez Activer Multi-Attach.
9. Pour le chiffrement, la valeur par défaut dépend du volume source et des paramètres de votre compte. Pour les copies du même compte, la copie hérite de la clé de chiffrement du volume source. Pour les copies entre comptes, la clé de cryptage Amazon EBS par défaut de votre compte est utilisée. Vous pouvez choisir une autre clé gérée par le client.
10. (Facultatif) Pour attribuer des balises personnalisées à la copie du volume, dans la section Balises, choisissez Ajouter une balise, puis entrez une paire clé-valeur de balise.
11. Choisissez Copier le volume.
12. Le volume copié entre dans `creating` cet état, puis passe à l'`available` état suivant. Vous pouvez ensuite l'associer à une instance Amazon EC2 dans la même zone de disponibilité.

AWS CLI

Pour copier un volume

Utilisez la commande [copy-volumes](#).

L'exemple suivant crée une copie de volume de `vol-01234567890abcdef` avec le type de `gp3` volume, une taille de 100 GiB et un débit de 250 MiB/s.

```
aws ec2 copy-volumes \  
--source-volume-id vol-01234567890abcdef \  
--volume-type gp3 \  
--size 100 \  
--throughput 250
```

Pour chiffrer un volume non chiffré pendant la copie

Utilisez la commande `copy-volumes` avec les paramètres `--encrypted` et `--kms-key-id`.

```
aws ec2 copy-volumes \  
--source-volume-id vol-01234567890abcdef \  
--encrypted \  
--kms-key-id alias/my-key
```

Pour rechiffrer à l'aide d'une autre clé gérée par le client

Utilisez la commande `copy-volumes` avec le `--kms-key-id` paramètre pour spécifier une clé différente.

```
aws ec2 copy-volumes \  
--source-volume-id vol-01234567890abcdef \  
--kms-key-id arn:aws:kms:us-east-1:222222222222:key/abcd1234-a123-456a-a12b-a123b4cd56ef
```

PowerShell

Pour copier un volume

Utilisez l'applet de commande [Copy-EC2Volume](#).

L'exemple suivant crée une copie de volume de `vol-01234567890abcdef` avec le type de `gp3` volume, une taille de 100 GiB et un débit de 250 MiB/s.

```
Copy-EC2Volume `
```

```
-SourceVolumeId vol-01234567890abcdef `
-VolumeType gp3 `
-Size 100 `
-Throughput 250
```

Pour chiffrer un volume non chiffré pendant la copie

Utilisez l' `Copy-EC2Volume` applet de commande avec les paramètres `-Encrypted` et `-KmsKeyId`

```
Copy-EC2Volume `
-SourceVolumeId vol-01234567890abcdef `
-Encrypted $true `
-KmsKeyId "alias/my-key"
```

Pour rechiffrer à l'aide d'une autre clé gérée par le client

Utilisez l' `Copy-EC2Volume` applet de commande avec le `-KmsKeyId` paramètre pour spécifier une clé différente.

```
Copy-EC2Volume `
-SourceVolumeId vol-01234567890abcdef `
-KmsKeyId "arn:aws:kms:us-east-1:222222222222:key/abcd1234-a123-456a-a12b-a123b4cd56ef"
```

Attacher un volume Amazon EBS à une instance Amazon EC2

Vous pouvez attacher un volume EBS disponible à l'une de vos instances se trouvant dans la même zone de disponibilité que le volume.

Pour plus d'informations sur l'ajout de volumes EBS à votre instance lors du lancement, consultez la rubrique [Instance Block Device Mapping](#).

Considérations

- Le nombre maximum de volumes Amazon EBS que vous pouvez associer à une instance dépend du type d'instance. Si vous dépassez la limite de volume de pièces jointes pour un type d'instance, la demande de pièce jointe échoue avec le `AttachmentLimitExceeded` message d'erreur. Pour plus d'informations, consultez la section Limites de volume des [instances](#).

- Vous pouvez associer des volumes à des instances situées dans la même zone de disponibilité uniquement.
- Multi-Attach les volumes activés peuvent être attachés à un maximum de 16 instances. Pour plus d'informations, consultez [Attachez un volume EBS à plusieurs instances EC2 à l'aide de Multi-Attach](#).
- Si le volume comporte un code AWS Marketplace produit :
 - Vous ne pouvez l'associer qu'à une instance arrêtée.
 - Vous devez être abonné au AWS Marketplace code qui se trouve sur le volume.
 - La configuration de l'instance, comme son type et son système d'exploitation, doit prendre en charge ce AWS Marketplace code spécifique. Par exemple, vous ne pouvez pas prendre un volume sur une instance Windows et l'attacher à une instance Linux.
 - AWS Marketplace les codes sont copiés du volume vers l'instance.
- Ce nom d'appareil que vous spécifiez est utilisé par Amazon EC2. Le pilote de périphérique en mode bloc peut monter le périphérique avec un nom de périphérique différent de celui que vous avez spécifié. Pour plus d'informations, consultez la section Noms des [appareils pour les volumes sur les instances](#) Amazon EC2.
- Dans certains cas, un volume autre que le volume attaché à l'instance `/dev/xvda` ou `/dev/sda` pouvant devenir le volume racine de l'instance. Cela peut se produire si vous attachez le volume racine d'une autre instance, ou un volume créé à partir de l'instantané d'un volume racine, à une instance avec un volume racine existant. Pour plus d'informations, voir [Démarrer à partir du mauvais volume](#).
- Certains types d'instances prennent en charge plusieurs cartes EBS. Vous pouvez sélectionner la carte EBS pour le volume à connecter en spécifiant l'index de la carte EBS. Pour les instances prenant en charge plusieurs cartes EBS, voir Cartes [EBS](#).
 - Votre volume racine doit être associé à l'index 0 de la carte EBS.
 - Pour les instances qui prennent en charge plusieurs cartes EBS, si vous ne spécifiez pas l'index des cartes EBS, votre volume sera associé à l'index des cartes EBS. 0
 - Lorsque vous configurez vos instances EC2 pour des charges de travail hautes performances, il est essentiel d'équilibrer les volumes EBS entre les cartes EBS en fonction des exigences de performances, afin d'éviter de rencontrer des limites de performances sur l'une des cartes EBS.
 - La limite de volume de pièces jointes pour un type d'instance est répartie de manière égale sur chaque carte EBS. Par exemple, sur une instance EC2 qui prend en charge les pièces jointes de 128 volume avec deux cartes EBS, chaque carte EBS peut prendre en charge jusqu'à 64 des

pièces jointes de volume. Si vous dépassez la limite de pièces jointes par carte EBS, la demande échoue avec le `CardAttachmentLimitExceeded` message d'erreur.

Console

Pour associer un volume EBS à une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume à attacher et choisissez Actions, Attach volume (Attacher un volume).
4. Pour Instance, saisissez l'ID de l'instance ou sélectionnez l'instance dans la liste d'options.
5. Pour Nom de l'appareil, effectuez l'une des opérations suivantes :
 - Pour un volume racine, sélectionnez le nom de périphérique requis dans la section Réserve au volume racine de la liste. Généralement `/dev/sda1` ou `/dev/xvda` pour les instances Linux en fonction de l'AMI, ou `/dev/sda1` pour les instances Windows.
 - Pour les volumes de données, sélectionnez un nom d'appareil disponible dans la section Recommandé pour les volumes de données de la liste.
 - Pour utiliser un nom d'appareil personnalisé, sélectionnez Spécifier un nom d'appareil personnalisé, puis entrez le nom de l'appareil à utiliser.
6. Choisissez Attacher un volume.
7. Connectez-vous à votre instance et montez le volume. Pour plus d'informations, consultez [Mettre un volume Amazon EBS à disposition pour utilisation](#).

AWS CLI

Pour associer un volume EBS à une instance

Utilisez la commande [attach-volume](#). L'exemple suivant associe le volume spécifié à l'instance spécifiée en utilisant le nom de périphérique spécifié.

```
aws ec2 attach-volume \  
  --volume-id vol-01234567890abcdef \  
  --instance-id i-1234567890abcdef0 \  
  --device /dev/sdf
```

PowerShell

Pour associer un volume EBS à une instance

Utilisez l'applet de commande [Add-EC2Volume](#). L'exemple suivant associe le volume spécifié à l'instance spécifiée en utilisant le nom de périphérique spécifié.

```
Add-EC2Volume `
  -VolumeId vol-01234567890abcdef `
  -InstanceId i-1234567890abcdef0 `
  -Device /dev/sdf
```

Attachez un volume EBS à plusieurs instances EC2 à l'aide de Multi-Attach

Amazon EBS vous Multi-Attach permet d'associer un seul SSD (io1 ou io2) volume IOPS provisionné à plusieurs instances situées dans la même zone de disponibilité. Vous pouvez associer plusieurs volumes Multi-Attach activés à une instance ou à un ensemble d'instances. Chaque instance à laquelle le volume est attaché dispose des autorisations de lecture et d'écriture complètes sur le volume partagé. Multi-Attach vous permet d'améliorer plus facilement la disponibilité des applications qui gèrent des opérations d'écriture simultanées.

Tarification et facturation

L'utilisation d'Amazon EBS Multi-Attach est gratuite. Vous êtes facturé selon les frais standard qui s'appliquent aux volumes SSD IOPS provisionnés (io1 et io2). Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Table des matières

- [Considérations et restrictions](#)
- [Performances pour les Multi-Attach volumes Amazon EBS](#)
- [Activer Multi-Attach pour un volume Amazon EBS](#)
- [Désactiver Multi-Attach pour un volume Amazon EBS](#)
- [Utiliser les réservations NVMe avec les Multi-Attach volumes Amazon EBS activés](#)

Considérations et restrictions

- Multi-Attach les volumes activés peuvent être attachés à un maximum de 16 instances créées sur le système [Nitro et](#) situées dans la même zone de disponibilité.

- Les instances Linux prennent en charge io1 les io2 volumes et Multi-Attach activés. Les instances Windows ne prennent en charge que io2 les volumes Multi-Attach activés.
- Le nombre maximal de volumes Amazon EBS que vous pouvez associer à une instance dépend du type et de la taille de l'instance. Pour plus d'informations, consultez la section Limites de volume des [instances](#).
- Multi-Attach est pris en charge exclusivement sur les [volumes SSD \(io1etio2\) IOPS provisionnés](#).
- Multi-Attach pour les io1 volumes est disponible dans toutes les régions qui le prennent en chargeio1.

Multi-Attach for io2 est disponible dans toutes les régions qui prennent en chargeio2.

 Note

Pour améliorer les performances, la cohérence et la durabilité à moindre coût, nous vous recommandons d'utiliser des volumes io2.

- Les systèmes de fichiers standards, tels que XFS et EXT4, ne sont pas conçus pour être accessibles simultanément par plusieurs serveurs, tels que les instances EC2. Vous devez utiliser un système de fichiers en cluster pour vous assurer que vos données sont résilientes et fiables pour vos charges de travail de production.
- Multi-Attach activé io1 et les io2 volumes supportent les I/O clôtures. I/O les protocoles de clôture contrôlent l'accès en écriture dans un environnement de stockage partagé afin de maintenir la cohérence des données. Vos applications doivent fournir un ordre d'écriture pour les instances attachées afin de maintenir la cohérence des données. Pour plus d'informations, consultez [Utiliser les réservations NVMe avec les Multi-Attach volumes Amazon EBS activés](#).
- Multi-Attach les volumes activés ne peuvent pas être créés en tant que volumes de démarrage.
- Multi-Attach les volumes activés peuvent être attachés à un mappage de périphériques en mode bloc par instance.
- Multi-Attach ne peut pas être activé lors du lancement de l'instance à l'aide de la console Amazon EC2 ou de RunInstances l'API.
- Multi-Attach les volumes activés qui présentent un problème au niveau de la couche d'infrastructure Amazon EBS ne sont pas disponibles pour toutes les instances connectées. Des problèmes au niveau de la couche Amazon EC2 ou de mise en réseau peuvent affecter seulement certaines instances attachées.

- Le tableau suivant indique la prise en charge de la modification des volumes pour les volumes Multi-Attach activés `io1` et `io2` les volumes après leur création.

	io2 Volumes	io1 Volumes
Modifier le type de volume	✓ **	✓ **
Modifier la taille du volume	✓	✓
Modifier les IOPS provisionnés	✓	✓
Activer Multi-Attach	✓ *	✓ *
Désactiver Multi-Attach	✓ *	✓ *

* Vous ne pouvez ni activer ni désactiver le volume Multi-Attach lorsque celui-ci est attaché à une instance.

** La modification du type de volume pour les volumes Multi-Attach activés n'est prise en charge qu'entre `io1` et `io2`, dans les deux sens, y compris lorsque le volume est connecté. Les autres modifications de type de volume ne sont pas prises en charge.

- Multi-Attach les volumes activés sont supprimés lors de la fermeture de l'instance si la dernière instance attachée est terminée et si cette instance est configurée pour supprimer le volume à la fermeture. Si le volume est attaché à plusieurs instances présentant des paramètres de suppression à la résiliation différents dans leurs mappages de périphérique de stockage en mode bloc, le paramètre de mappage de périphériques de bloc de la dernière instance attachée détermine le comportement de suppression à la résiliation.

Pour garantir un comportement prévisible en matière de suppression à la résiliation, activez ou désactivez la suppression à la résiliation pour toutes les instances auxquelles le volume est

attaché. Pour plus d'informations, consultez la section [Conserver les données lorsqu'une instance est arrêtée](#).

- Vous pouvez surveiller un volume Multi-Attach activé à l'aide des CloudWatch métriques pour les volumes Amazon EBS. Les données sont agrégées dans toutes les instances attachées. Vous ne pouvez pas surveiller les métriques pour des instances individuelles attachées. Pour plus d'informations, consultez [Statistiques CloudWatch Amazon pour Amazon EBS](#).

Performances pour les Multi-Attach volumes Amazon EBS

Chaque instance attachée est capable de piloter ses performances IOPS maximales jusqu'aux performances provisionnées maximales du volume. Toutefois, les performances agrégées de toutes les instances attachées ne peuvent pas dépasser les performances provisionnées maximales du volume. Si la demande d'IOPS des instances attachées est supérieure aux IOPS provisionnées du volume, le volume ne dépassera pas ses performances provisionnées.

Supposons, par exemple, que vous créiez un volume `io2` Multi-Attach activé avec des IOPS 80,000 provisionnées et que vous l'associez à une `m7g.large` instance qui prend en charge jusqu'à 40,000 IOPS et à une `r7g.12xlarge` instance qui prend en charge jusqu'à IOPS. 60,000. Chaque instance peut gérer ses IOPS maximum car la valeur est inférieure aux IOPS provisionnés () du volum 80,000. Toutefois, si les deux instances accèdent simultanément I/O au volume, leurs IOPS combinées ne peuvent pas dépasser les performances IOPS provisionnées du 80,000 volume.

Pour obtenir des performances constantes, il est recommandé d'équilibrer les I/O commandes provenant d'instances attachées entre les secteurs d'un volume Multi-Attach activé.

Pour plus d'informations sur les performances IOPS pour les types d'instance Amazon EC2, consultez la section Types d'instance optimisés pour [Amazon EBS](#) dans le guide de l'utilisateur Amazon EC2.

Activer Multi-Attach pour un volume Amazon EBS

Multi-Attach les volumes activés peuvent être gérés de la même manière que vous géreriez n'importe quel autre volume Amazon EBS. Toutefois, pour utiliser cette Multi-Attach fonctionnalité, vous devez l'activer pour le volume.

Lorsque vous créez un nouveau volume, elle Multi-Attach est désactivée par défaut. Vous pouvez l'activer Multi-Attach lorsque vous créez un volume.

Vous pouvez également activer Multi-Attach les **io2** volumes **for io1** et après leur création, mais uniquement s'ils ne sont attachés à aucune instance.

Après avoir activé Multi-Attach un volume, vous pouvez l'associer à une instance de la même manière que vous attachez n'importe quel autre volume EBS. Pour plus d'informations, consultez [Attacher un volume Amazon EBS à une instance Amazon EC2](#).

Console

À activer Multi-Attach lors de la création du volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Choisissez Créer un volume.
4. Pour Type de volume, sélectionnez SSD IOPS provisionnés (**io1**) ou SSD IOPS provisionnés (**io2**).
5. Pour Size (Taille) et IOPS, choisissez la taille de volume requise et le nombre d'I/O par seconde à provisionner.
6. Pour Availability Zone (Zone de disponibilité), choisissez la même zone de disponibilité que celle dans laquelle se trouvent les instances.
7. Pour Amazon EBS Multi-Attach, choisissez Activer Multi-Attach.
8. (Facultatif) Pour Snapshot ID (ID d'instantané), choisissez l'instantané à partir duquel créer le volume.
9. Définissez l'état du chiffrement du volume.

Si l'instantané sélectionné est chiffré, ou si votre compte est activé pour le [chiffrement par défaut](#), le chiffrement est activé automatiquement et vous ne pouvez pas le désactiver. Vous pouvez choisir la clé KMS à utiliser pour chiffrer le volume.

Si l'instantané sélectionné n'est pas chiffré et que le chiffrement par défaut n'est pas activé pour votre compte, le chiffrement est facultatif. Pour chiffrer le volume, pour Encryption (Chiffrement), choisissez Encrypt this volume (Chiffrer ce volume), puis sélectionnez la clé KMS à utiliser pour chiffrer le volume.

Vous ne pouvez attacher des volumes chiffrés qu'aux instances qui prennent en charge le chiffrement Amazon EBS. Pour plus d'informations, consultez [Chiffrement Amazon EBS](#).

10. (Facultatif) Pour attribuer des identifications personnalisées au volume, dans la section Tags (Identifications), choisissez Add tag (Ajouter une identification), puis saisissez une paire clé-valeur d'identification.
11. Choisissez Créer un volume.

À activer Multi-Attach après la création

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume, puis Actions et Modify volume (Modifier un volume).
4. Pour Amazon EBS Multi-Attach, choisissez Activer Multi-Attach.
5. Sélectionnez Modifier.

AWS CLI

À activer Multi-Attach lors de la création du volume

Utilisez la [commande](#) create-volume avec l'option `--multi-attach-enabled`.

```
aws ec2 create-volume \
  --volume-type io2 \
  --multi-attach-enabled \
  --size 100 \
  --iops 2000 \
  --region us-west-2 \
  --availability-zone us-west-2b
```

À activer Multi-Attach après la création

Utilisez la [commande](#) modify-volume avec l'option `--multi-attach-enabled`.

```
aws ec2 modify-volume \
  --volume-id vol-01234567890abcdef \
  --multi-attach-enabled
```

PowerShell

À activer Multi-Attach lors de la création du volume

Utilisez l'[New-EC2Volume](#) applet de commande avec le `-MultiAttachEnabled` paramètre.

```
New-EC2Volume `
  -VolumeType io2 `
  -MultiAttachEnabled $true `
  -Size 100 `
  -Iops 2000 `
  -Region us-west-2 `
  -AvailabilityZone us-west-2b
```

À activer Multi-Attach après la création

Utilisez l'[Edit-EC2Volume](#) applet de commande avec le `-MultiAttachEnabled` paramètre.

```
Edit-EC2Volume `
  -VolumeId vol-01234567890abcdef `
  -MultiAttachEnabled $true
```

Désactiver Multi-Attach pour un volume Amazon EBS

Vous ne pouvez le désactiver que Multi-Attach pour un io2 volume io1 ou s'il n'est pas attaché à une instance.

Console

À désactiver Multi-Attach après la création

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume, puis Actions et Modify volume (Modifier un volume).
4. Pour Amazon EBS Multi-Attach, désactivez Activer Multi-Attach.
5. Sélectionnez Modifier.

AWS CLI

À désactiver Multi-Attach après la création

Utilisez la [commande](#) `modify-volume` avec l'option `-no-multi-attach-enabled`

```
aws ec2 modify-volume \  
  --volume-id vol-01234567890abcdef \  
  --no-multi-attach-enabled
```

PowerShell

À désactiver Multi-Attach après la création

Utilisez l'[Edit-EC2Volume](#) applet de commande avec le `-MultiAttachEnabled` paramètre.

```
Edit-EC2Volume \  
  -VolumeId vol-01234567890abcdef \  
  -MultiAttachEnabled $false
```

Utiliser les réservations NVMe avec les Multi-Attach volumes Amazon EBS activés

Multi-Attach activé `io1` et les `io2` volumes prennent en charge les réservations NVMe, qui est un ensemble de protocoles de séparation de stockage standard. Ces protocoles vous permettent de créer et de gérer des réservations qui contrôlent et coordonnent l'accès de plusieurs instances à un volume partagé. Les applications de stockage partagé utilisent des réservations pour garantir la cohérence des données.

Table des matières

- [Exigences](#)
- [Activer la prise en charge des réservations NVMe](#)
- [Commandes de réservations NVMe prises en charge](#)
- [Tarification](#)

Exigences

Les réservations NVMe sont prises en charge avec les commandes Multi-Attach activées `io1` et les `io2` volumes. Multi-Attach les volumes activés ne peuvent être attachés qu'à des instances créées sur le système Nitro.

Les réservations NVMe sont prises en charge avec les systèmes d'exploitation suivants :

- SUSE Linux Enterprise 12 SP3 ou version ultérieure

- RHEL 8.3 et versions ultérieures
- Amazon Linux 2 et versions ultérieures
- Windows Server 2016 et versions ultérieures

 Note

Pour les AMI Windows Server prises en charge datées du 13.09.2023 et ultérieures, les pilotes NVMe requis sont inclus. Pour les AMI antérieures, vous devez passer à la version 1.5.0 ou une version ultérieure du pilote NVMe. Pour plus d'informations, consultez la section Pilotes [AWS NVMe](#).

Si vous utilisez EC2Launch v2 pour initialiser vos disques, vous devez effectuer une mise à niveau vers la version 2.0.1521 ou ultérieure. Pour plus d'informations, consultez la section [Utiliser l'agent EC2Launch v2](#).

Activer la prise en charge des réservations NVMe

La prise en charge des réservations NVMe est activée par défaut pour tous les io2 volumes Multi-Attach activés créés après le 18 septembre 2023 et pour tous les io1 volumes Multi-Attach activés créés après le 1er octobre 2026.

Pour activer la prise en charge des réservations NVMe pour les io2 volumes existants créés avant le 18 septembre 2023 ou les io1 volumes existants créés avant le 1er octobre 2026, vous devez détacher toutes les instances du volume, puis rattacher les instances requises. Les réservations NVMe seront activées pour tous les attachements créés après le détachement de toutes les instances.

Commandes de réservations NVMe prises en charge

Amazon EBS prend en charge les commandes de réservations NVMe suivantes :

Reservation Register

Enregistre, annule ou remplace une clé de réservation. Une clé d'enregistrement est utilisée pour identifier et authentifier une instance. L'enregistrement d'une clé de réservation auprès d'un volume crée une association entre l'instance et le volume. Vous devez enregistrer l'instance auprès du volume pour qu'elle puisse obtenir une réservation.

Reservation Acquire

Acquiert une réservation sur un volume, anticipe une réservation enregistrée sur un espace de noms et annule une réservation enregistrée sur un volume. Les types de réservation suivants peuvent être acquis :

- Réservation Write Exclusive
- Réservation Exclusive Access
- Réservation Write Exclusive - Registrants Only
- Réservation Exclusive Access - Registrants Only
- Réservation Write Exclusive - All Registrants
- Réservation Exclusive Access - All Registrants

Reservation Release

Publie ou efface une réservation enregistrée sur un volume.

Reservation Report

Décrit le statut d'enregistrement et de réservation d'un volume.

Tarification

Il n'y a aucun coût supplémentaire pour l'activation et l'utilisation Multi-Attach.

Mettre un volume Amazon EBS à disposition pour utilisation

Une fois que vous avez attaché un volume Amazon EBS à votre instance, il est exposé en tant que périphérique de blocage. Vous pouvez formater le volume avec n'importe quel système de fichiers puis le monter. Après avoir rendu le volume EBS disponible à l'utilisation, vous pouvez y accéder de la même façon que n'importe quel volume. Toutes les données inscrites sur ce système de fichiers le sont sur le volume EBS et sont transparentes pour les applications utilisant cet appareil.

Vous pouvez prendre des instantanés de votre volume EBS à des fins de sauvegarde ou pour servir de base à la création d'un autre volume. Pour plus d'informations, consultez [Instantanés Amazon EBS](#).

Si le volume EBS que vous préparez à utiliser est supérieur à 2 Tio, vous devez utiliser un schéma de partitionnement GPT pour accéder à l'ensemble du volume. Pour plus d'informations, consultez [Contraintes de volume Amazon EBS](#).

Instances Linux

Formatage et montage d'un volume attaché

Supposons que vous ayez une instance EC2 avec un volume EBS pour le périphérique racine, `/dev/xvda`, et que vous venez d'attacher un volume EBS vide à l'instance en utilisant `/dev/sdf`. Utilisez la procédure suivante pour mettre le volume nouvellement attaché à disposition.

Pour formater et monter un volume EBS sous Linux

1. Connectez-vous à votre instance à l'aide de SSH. Pour plus d'informations, consultez la section [Connexion à votre instance Linux](#).
2. Le périphérique peut être attaché à l'instance avec un nom de périphérique différent de celui que vous avez spécifié dans le mappage de périphérique de stockage en mode bloc. Pour plus d'informations, consultez la section Noms des [périphériques sur les instances Linux](#). Utilisez la commande `lsblk` pour voir vos périphériques de disques disponibles et leurs points de montage (le cas échéant) pour vous aider à déterminer quel nom d'appareil utiliser. Le résultat de `lsblk` supprime le préfixe `/dev/` des chemins d'accès complets à l'appareil.

Voici un exemple de sortie pour une instance construite sur le système [Nitro](#), qui expose les volumes EBS sous forme de périphériques de bloc NVMe. Le périphérique racine est `/dev/nvme0n1`, et il possède deux partitions nommées `nvme0n1p1` et `nvme0n1p128`. Le volume attaché est `/dev/nvme1n1`, et il ne dispose pas de partition ni n'est encore monté.

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  10G  0 disk
nvme0n1       259:1    0   8G  0 disk
-nvme0n1p1    259:2    0   8G  0 part /
-nvme0n1p128  259:3    0   1M  0 part
```

L'exemple ci-dessous représente la sortie pour une instance T2. Le périphérique racine est `/dev/xvda`, et il possède une partition nommée `xvda1`. Le volume attaché est `/dev/xvdf`, et il ne dispose pas de partition ni n'est encore monté.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda      202:0    0   8G  0 disk
-xvda1    202:1    0   8G  0 part /
```



```
xvdf    202:80    0    10G    0 disk
```

- Déterminez s'il y a un système de fichiers sur le volume. Les nouveaux volumes sont des périphériques de stockage en mode bloc bruts et vous devez créer un système de fichiers sur ces volumes avant de pouvoir les monter et les utiliser. Les volumes créés à partir d'instantanés disposent probablement déjà d'un système de fichiers. Si vous créez un autre système de fichiers par-dessus le système de fichiers existant, l'opération remplace vos données.

Utilisez l'une des méthodes suivantes ou les deux pour déterminer s'il existe un système de fichiers sur le volume :

- Utilisez la commande `file -s` pour obtenir les informations sur un appareil spécifique, telles que son type de système de fichiers. Si le résultat de la commande précédente est simplement `data`, comme dans l'exemple de sortie suivant, il n'y a pas de système de fichiers sur l'appareil.

```
[ec2-user ~]$ sudo file -s /dev/xvdf
/dev/xvdf: data
```

Si l'appareil possède un système de fichiers, la commande affiche des informations sur le type de système de fichiers. Par exemple, la sortie suivante montre un périphérique racine avec le système de fichiers XFS.

```
[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: SGI XFS filesystem data (blksize 4096, inosize 512, v2 dirs)
```

- Utilisez la commande `lsblk -f` pour obtenir des informations sur tous les appareils attachés à l'instance.

```
[ec2-user ~]$ sudo lsblk -f
```

Par exemple, la sortie suivante montre qu'il y a trois appareils attachés aux instances —`nvme1n1`, `nvme0n1`, et `nvme2n1`. La première colonne répertorie les appareils et leurs partitions. La colonne `FSTYPE` indique le type de système de fichiers pour chaque appareil. Si la colonne est vide pour un appareil spécifique, cela signifie qu'il n'a pas de système de fichiers. Dans ce cas, l'appareil `nvme1n1` et la partition `nvme0n1p1` sur l'appareil `nvme0n1` sont tous deux formatés à l'aide du système de fichiers XFS, tandis que l'appareil `nvme2n1` et la partition `nvme0n1p128` sur l'appareil `nvme0n1` ne disposent pas de systèmes de fichiers.

```

NAME   FSTYPE LABEL  UUID                               MOUNTPOINT
nvme1n1          xfs    7f939f28-6dcc-4315-8c42-6806080b94dd
nvme0n1
##nvme0n1p1 xfs      / 90e29211-2de8-4967-b0fb-16f51a6e464c  /
##nvme0n1p128
nvme2n1

```

Si la sortie de ces commandes montre qu'il n'y a pas de système de fichiers sur l'appareil, vous devez en créer un.

4. (Condition) Si vous avez découvert qu'il y a un système de fichiers sur le périphérique à l'étape précédente, ignorez cette étape. Si vous avez un volume vide, utilisez la commande `mkfs -t` pour créer un système de fichiers sur le volume.

Warning

N'utilisez pas cette commande si vous montez un volume qui contient déjà des données (par exemple, un volume qui a été créé à partir d'un instantané). Sinon, vous formatez le volume et supprimerez les données existantes.

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
```

Si vous obtenez une erreur indiquant que `mkfs.xfs` est introuvable, utilisez la commande suivante pour installer les outils XFS, puis répétez la commande précédente :

```
[ec2-user ~]$ sudo yum install xfsprogs
```

5. Utilisez la commande `mkdir` pour créer un répertoire de point de montage pour le volume. Le point de montage est l'endroit où se trouve le volume dans l'arborescence du système de fichiers et où vous lisez et écrivez des fichiers après avoir monté le volume. L'exemple suivant crée un répertoire nommé `/data`.

```
[ec2-user ~]$ sudo mkdir /data
```

6. Montez le volume ou la partition dans le répertoire du point de montage que vous avez créé à l'étape précédente.

Si le volume ne comporte aucune partition, utilisez la commande suivante et spécifiez le nom du périphérique pour monter l'ensemble du volume.

```
[ec2-user ~]$ sudo mount /dev/xvdf /data
```

Si le volume comporte des partitions, utilisez la commande suivante et spécifiez le nom de la partition pour monter une partition.

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /data
```

7. Vérifiez les autorisations sur les fichiers de votre nouveau montage de volume pour vous assurer que les utilisateurs et les applications peuvent écrire sur le volume. Pour plus d'informations sur les autorisations sur les fichiers, consultez [File security](#) dans Le projet de documentation Linux.
8. Le point de montage n'est pas automatiquement préservé après le redémarrage de votre instance. Pour monter automatiquement ce volume EBS après le redémarrage, suivez la procédure suivante.

Monter automatiquement un volume attaché après le redémarrage

Pour monter un volume EBS attaché à chaque redémarrage du système, ajoutez une entrée pour l'appareil dans le fichier `/etc/fstab`.

Vous pouvez utiliser le nom du périphérique, comme `/dev/xvdf`, dans `/etc/fstab`, mais nous recommandons d'utiliser plutôt l'identificateur universel unique (UUID) de 128 bits de l'appareil. Les noms de périphériques peuvent changer, mais l'UUID persiste pendant toute la durée de vie de la partition. En utilisant l'UUID, vous réduisez les risques que le système devienne impossible à démarrer après une reconfiguration du matériel. Pour plus d'informations, consultez [Associer les volumes Amazon EBS aux noms des appareils NVMe](#).

Pour monter automatiquement un volume attaché après le redémarrage

1. (Facultatif) Créez une sauvegarde de votre fichier `/etc/fstab` que vous pouvez utiliser si vous détruisez ou supprimez accidentellement ce fichier en l'éditant.

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

2. Utilisez la commande `blkid` pour trouver l'UUID du périphérique. Notez l'UUID du périphérique que vous souhaitez monter après le redémarrage. Vous en aurez besoin à l'étape suivante.

Par exemple, la commande suivante indique que deux périphériques sont montés sur l'instance et affiche les UUID des deux périphériques.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

Pour Ubuntu 18.04, utilisez la commande `lsblk`.

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

3. Ouvrez le fichier `/etc/fstab` avec un éditeur de texte tel que `nano` ou `vim`.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

4. Ajoutez l'entrée suivante à `/etc/fstab` pour monter le périphérique au point de montage spécifié. Les champs sont la valeur UUID renvoyée par `blkid` (ou `lsblk` pour Ubuntu 18.04), le point de montage, le système de fichiers et les options de montage recommandées. Pour plus d'informations sur les champs obligatoires, exécutez `man fstab` pour ouvrir le manuel `fstab`.

L'exemple suivant monte le périphérique avec l'UUID sur le point `aebf131c-6957-451e-8d34-ec978d9581ae` de montage `/data` et utilise le système de fichiers `xfs`. Il utilise également les `nofail` drapeaux `defaults` et. Il spécifie `0` d'empêcher le vidage du système de fichiers et d'indiquer qu'il s'agit d'un périphérique non root. 2

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2
```

Note

Si jamais vous démarrez votre instance sans ce volume attaché (par exemple, après avoir déplacé ce volume sur une autre instance), l'option de montage `nofail` permet à l'instance de démarrer même si des erreurs se produisent lors du montage du volume. Les dérivés Debian, y compris les versions Ubuntu antérieures à 16.04, doivent également ajouter l'option de montage `nobootwait`.

5. Pour vérifier que votre entrée fonctionne, exécutez les commandes suivantes pour démonter le périphérique, puis montez tous les systèmes de fichiers dans `/etc/fstab`. S'il n'y a

pas d'erreur, le fichier `/etc/fstab` est correct et votre système de fichiers sera monté automatiquement après avoir été redémarré.

```
[ec2-user ~]$ sudo umount /data  
[ec2-user ~]$ sudo mount -a
```

Si vous recevez un message d'erreur, traitez les erreurs dans le fichier.

Warning

Des erreurs dans le fichier `/etc/fstab` peuvent rendre un système impossible à démarrer. N'arrêtez pas un système dont le fichier `/etc/fstab` contient des erreurs.

Si vous n'êtes pas sûr de savoir comment corriger des erreurs dans `/etc/fstab` et que vous avez créé un fichier de sauvegarde lors de la première étape de la procédure, vous avez toujours la possibilité de restaurer votre fichier depuis votre fichier de sauvegarde avec la commande suivante.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

instances Windows

Utilisez l'une des méthodes suivantes pour rendre un volume disponible sur une instance Windows.

PowerShell

Pour rendre tous les volumes EBS contenant des partitions brutes disponibles pour une utilisation avec Windows PowerShell

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez la section [Connexion à votre instance Windows](#).
2. Dans la barre des tâches, ouvrez le menu Démarrer et choisissez Windows PowerShell.
3. Utilisez la série de PowerShell commandes Windows fournie dans l'invite PowerShell ouverte. Le script effectue les actions suivantes par défaut :
 1. Met fin au service ShellHWDetection.
 2. Énumère les disques sur lesquels le style de partition est brut.

3. Crée une nouvelle partition qui couvre la taille maximale prise en charge par le disque et le type de partition.
4. Attribue une lettre de lecteur disponible.
5. Formate le système de fichiers en NTFS avec l'étiquette de système de fichiers spécifiée.
6. Redémarre le service ShellHWDetection.

```
Stop-Service -Name ShellHWDetection
Get-Disk | Where PartitionStyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
- PassThru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -
FileSystem NTFS -NewFileSystemLabel "Volume Label" -Confirm:$false
Start-Service -Name ShellHWDetection
```

DiskPart command line tool

Pour rendre un volume EBS disponible à l'aide de l'outil de ligne de DiskPart commande

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez la section [Connexion à votre instance Windows](#).
2. Déterminez le numéro de disque que vous souhaitez rendre disponible :
 1. Ouvrez le menu Démarrer, puis sélectionnez Windows PowerShell.
 2. Utilisez Get-Disk Cmdlet de commande pour récupérer une liste de disques disponibles.
 3. Dans la sortie de la commande, notez laNumérocorrespondant au disque que vous rendez disponible.
3. Créez un fichier de script pour exécuter DiskPart des commandes :
 1. Ouvrez le menu Démarrer et sélectionnezExplorer de fichiers.
 2. Accédez à un répertoire, tel que C:\, pour stocker le fichier de script.
 3. Choisissez (cliquez avec le bouton droit) sur un espace vide dans le dossier pour ouvrir la boîte de dialogue, placez le curseur sur Nouveau pour accéder au menu contextuel, puis choisissez Document texte.
 4. Nommez le fichier texte diskpart.txt.
4. Ajoutez les commandes suivantes au fichier script. Vous devrez peut-être modifier le numéro de disque, le type de partition, l'étiquette du volume et la lettre du lecteur. Le script effectue les actions suivantes par défaut :

1. Sélectionne le disque 1 pour modification.
2. Configure le volume pour utiliser la structure de partition MBR (Master Boot Record).
3. Formate le volume sous la forme d'un volume NTFS.
4. Définit l'étiquette du volume.
5. Attribue au volume une lettre de lecteur.

 Warning

Si vous montez un volume sur lequel se trouvent déjà des données, ne le reformatez pas, sinon vous supprimerez les données existantes.

```
select disk 1
attributes disk clear readonly
online disk noerr
convert mbr
create partition primary
format quick fs=ntfs label="volume_label"
assign letter="drive_letter"
```

Pour plus d'informations, voir [DiskPart Syntaxe et paramètres](#).

5. Ouvrez une invite de commande, accédez au dossier dans lequel se trouve le script et exécutez la commande suivante pour rendre un volume disponible sur le disque spécifié :

```
C:\> diskpart /s diskpart.txt
```

Disk Management utility

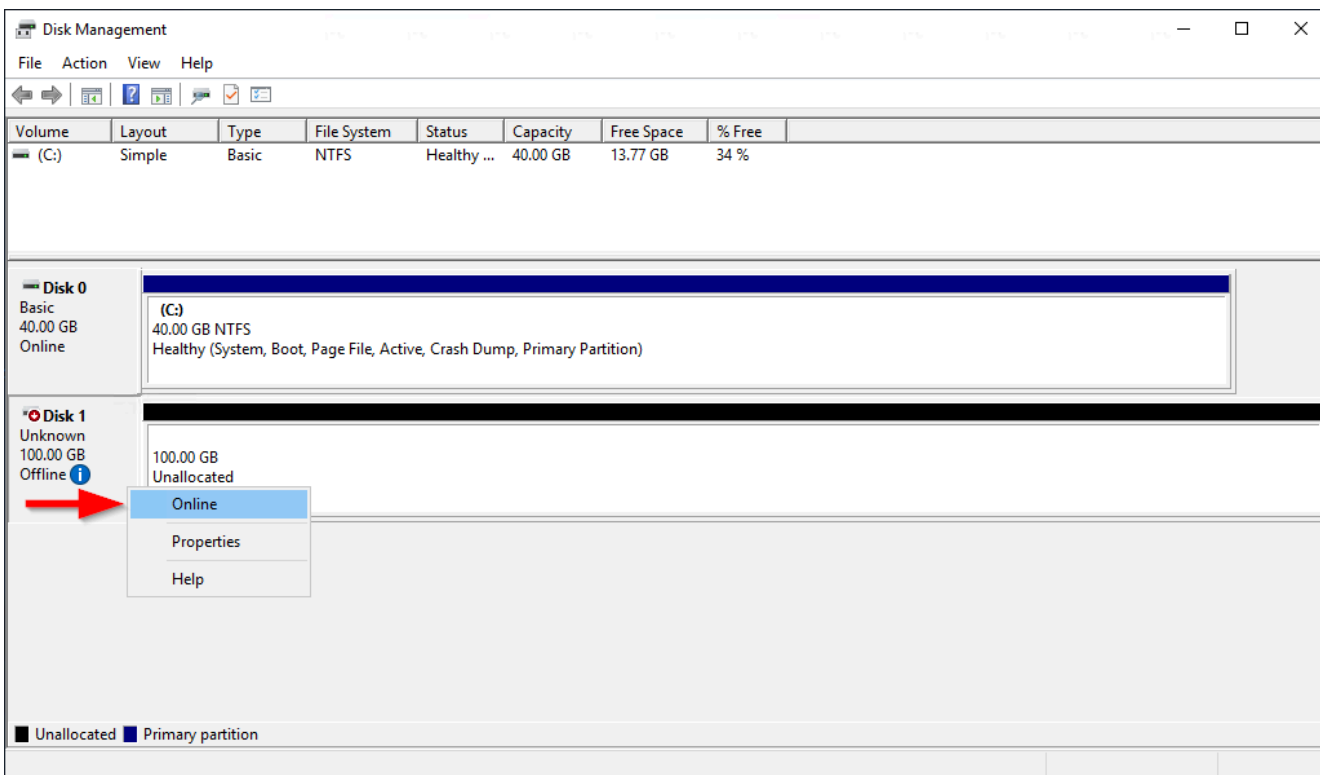
Pour rendre un volume EBS disponible à l'utilisation à l'aide de l'utilitaire Gestion des disques

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez la section [Connexion à votre instance Windows](#).
2. Démarrez l'utilitaire Gestion des disques. Dans la barre des tâches, ouvrez le menu contextuel (via un clic droit) du logo Windows et choisissez Gestion des disques.

Note

Sur Windows Server 2008, sélectionnez Démarrer, Outils d'administration, Gestion des ordinateurs et Gestion des disques.

3. Mettez le volume en ligne. Dans le volet inférieur, ouvrez le menu contextuel (avec un clic droit) du panneau de gauche associé au disque du volume EBS. Sélectionnez En ligne.



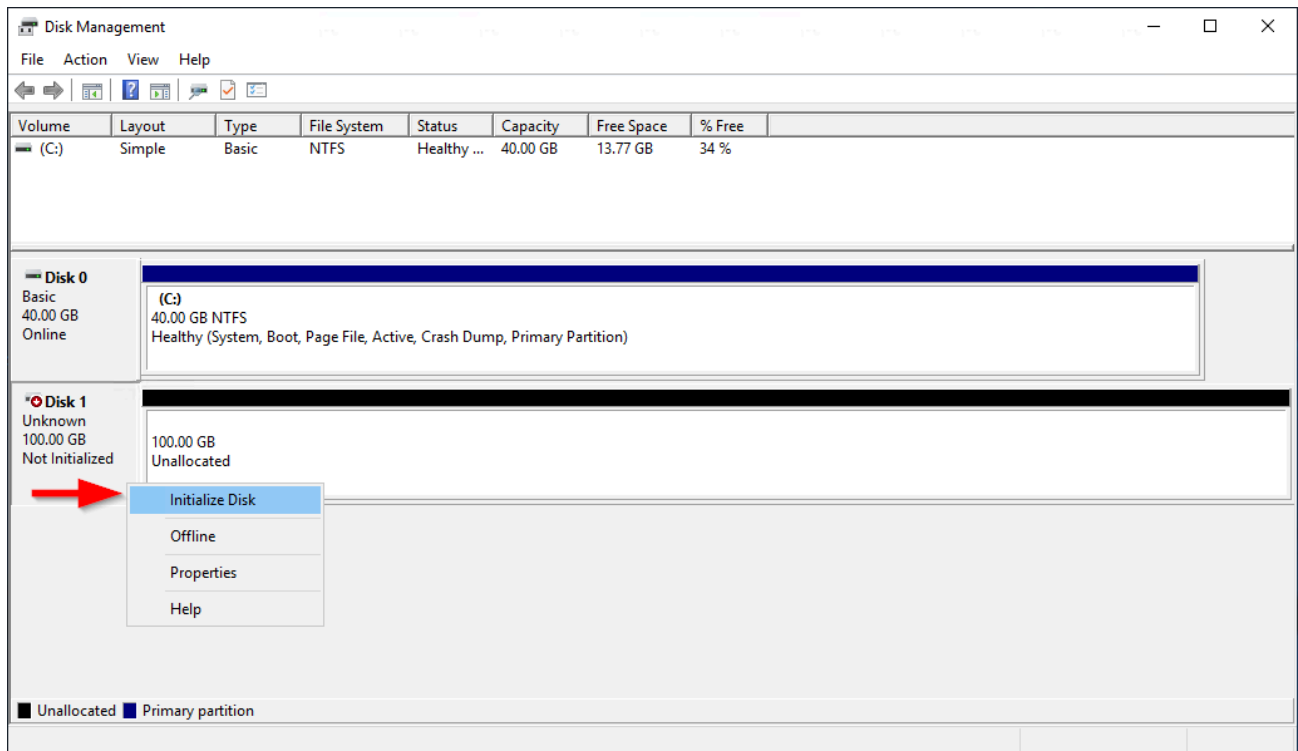
4. (Condition) Si le disque n'est pas initialisé, vous devez l'initialiser avant de pouvoir l'utiliser. Si le disque est déjà initialisé, ignorez cette étape.

Warning

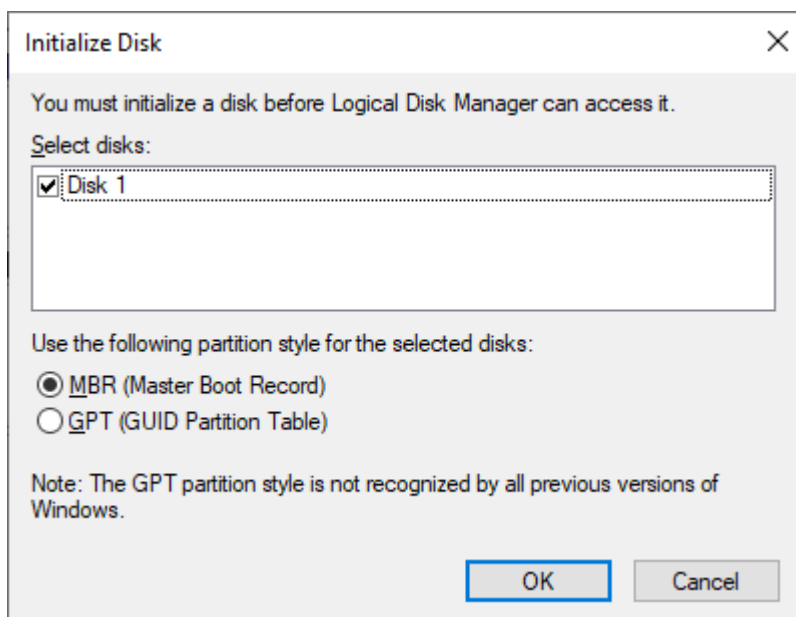
Si vous montez un volume sur lequel se trouvent déjà des données (par exemple, un ensemble de données public ou un volume créé à partir d'un instantané), ne le reformatez pas. Vous risqueriez de supprimer les données existantes.

Si le disque n'est pas initialisé, lancez-le comme suit :

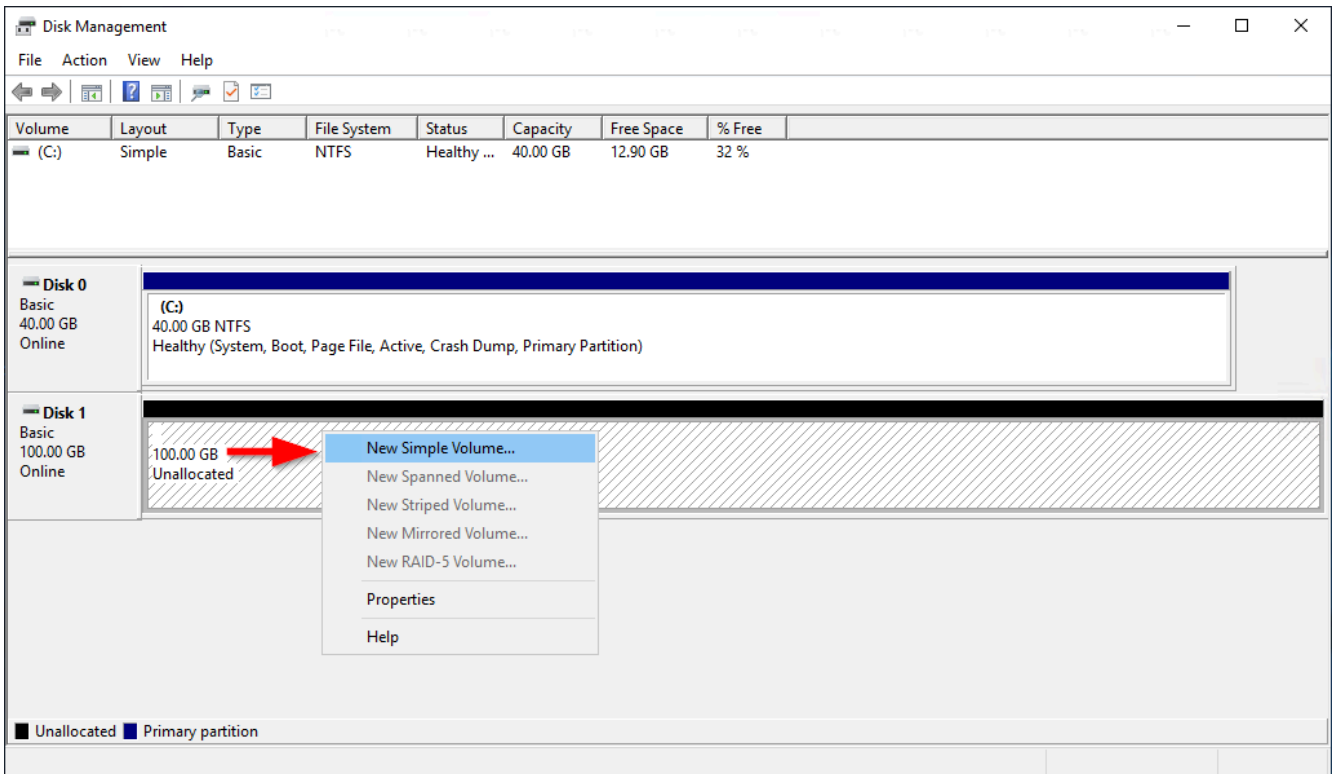
1. Ouvrez le menu contextuel (clic droit) du panneau de gauche du disque, et choisissez Initialiser le disque.



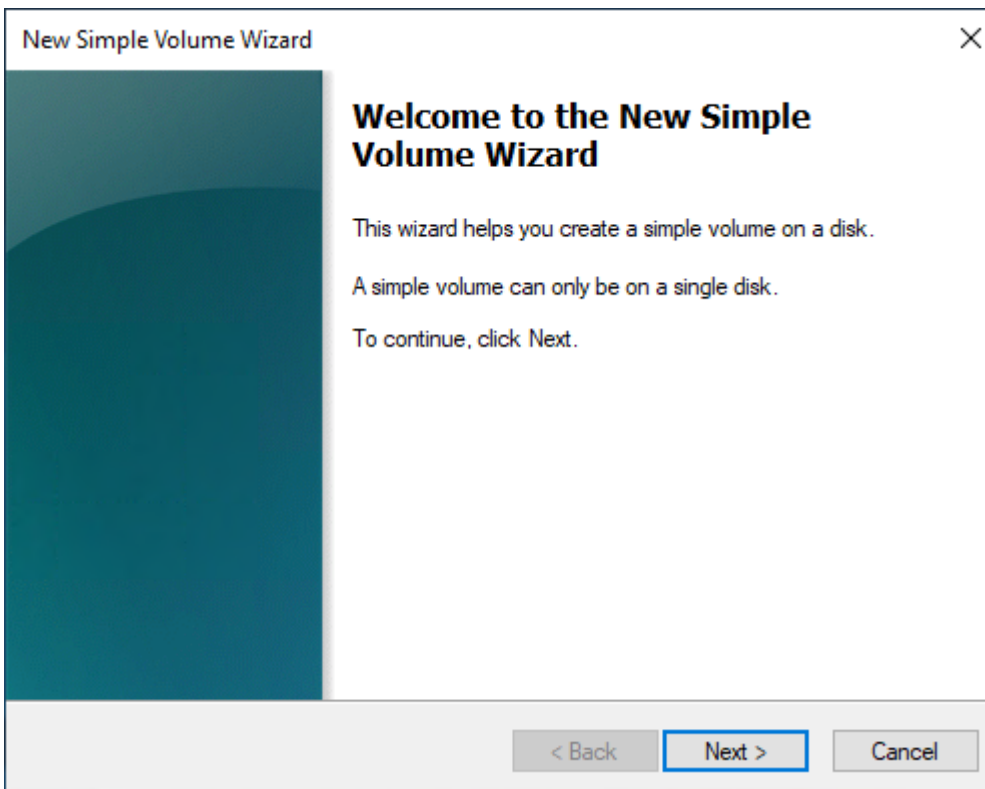
2. Dans la boîte de dialogue Initialiser le disque, sélectionnez un style de partition, puis appuyez sur OK.



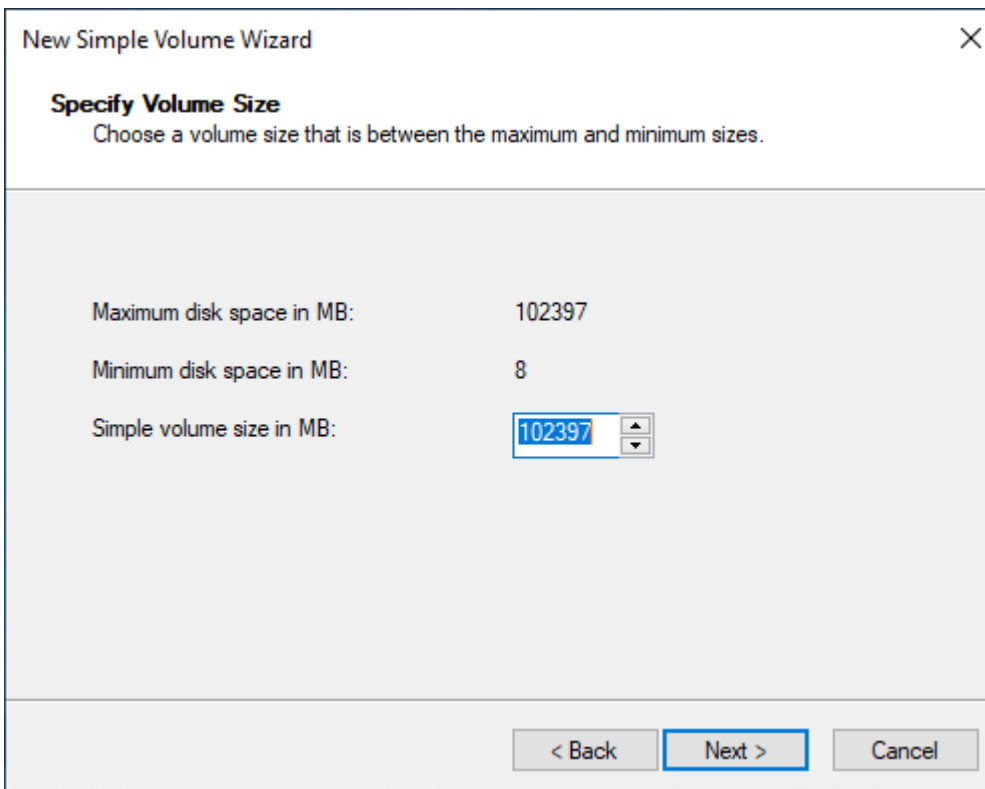
5. Ouvrez le menu contextuel (clic droit) du volet de droite du disque, puis appuyez sur Nouveau volume simple.



6. Dans l'Assistant Nouveau volume simple, choisissez Suivant.



7. Si vous souhaitez modifier la valeur maximale par défaut, spécifiez la valeur Taille simple du volume en Mo, puis choisissez Suivant.



The screenshot shows the 'Specify Volume Size' step of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the section is titled 'Specify Volume Size' with a subtitle 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three rows of information: 'Maximum disk space in MB:' with the value '102397', 'Minimum disk space in MB:' with the value '8', and 'Simple volume size in MB:' with a text box containing '102397' and a spinner control to its right. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

New Simple Volume Wizard

Specify Volume Size
Choose a volume size that is between the maximum and minimum sizes.

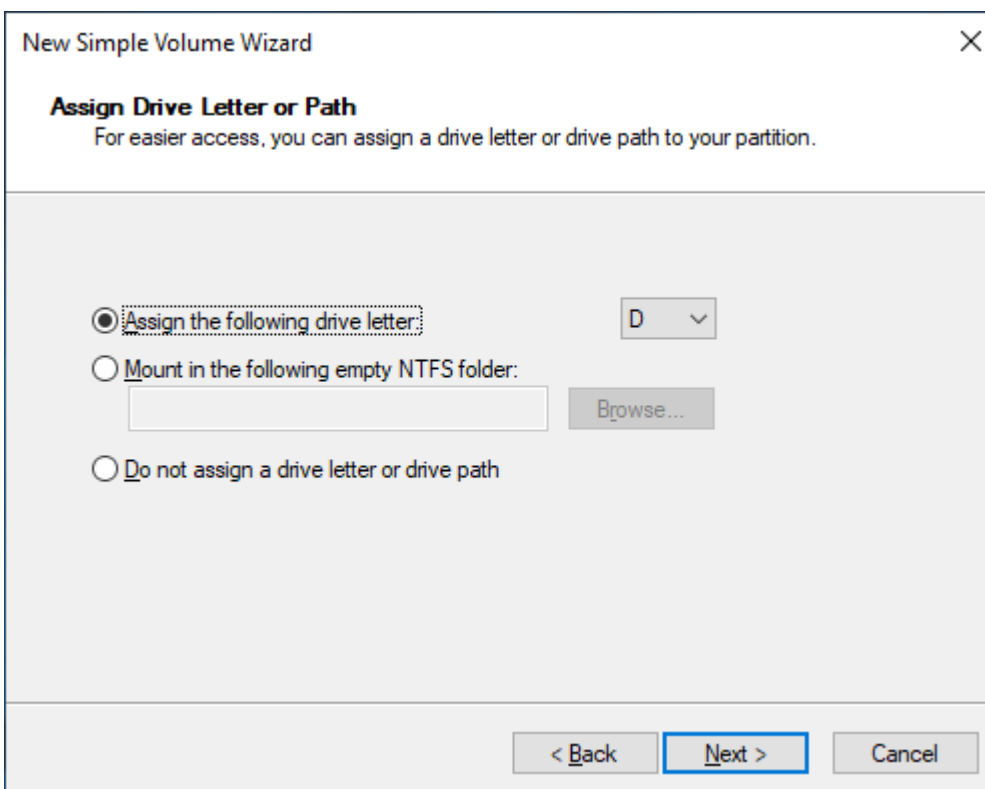
Maximum disk space in MB: 102397

Minimum disk space in MB: 8

Simple volume size in MB: 102397

< Back Next > Cancel

8. Spécifiez une lettre de lecteur préférée, si nécessaire, dans le menu déroulant. Attribuez la lettre de lecteur suivante, puis choisissez Suivant.



The screenshot shows the 'Assign Drive Letter or Path' step of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the section is titled 'Assign Drive Letter or Path' with a subtitle 'For easier access, you can assign a drive letter or drive path to your partition.' The main area contains three radio button options: 'Assign the following drive letter:' (selected), 'Mount in the following empty NTFS folder:', and 'Do not assign a drive letter or drive path'. The 'Assign the following drive letter:' option has a dropdown menu showing 'D'. The 'Mount in the following empty NTFS folder:' option has a text box and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

New Simple Volume Wizard

Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.

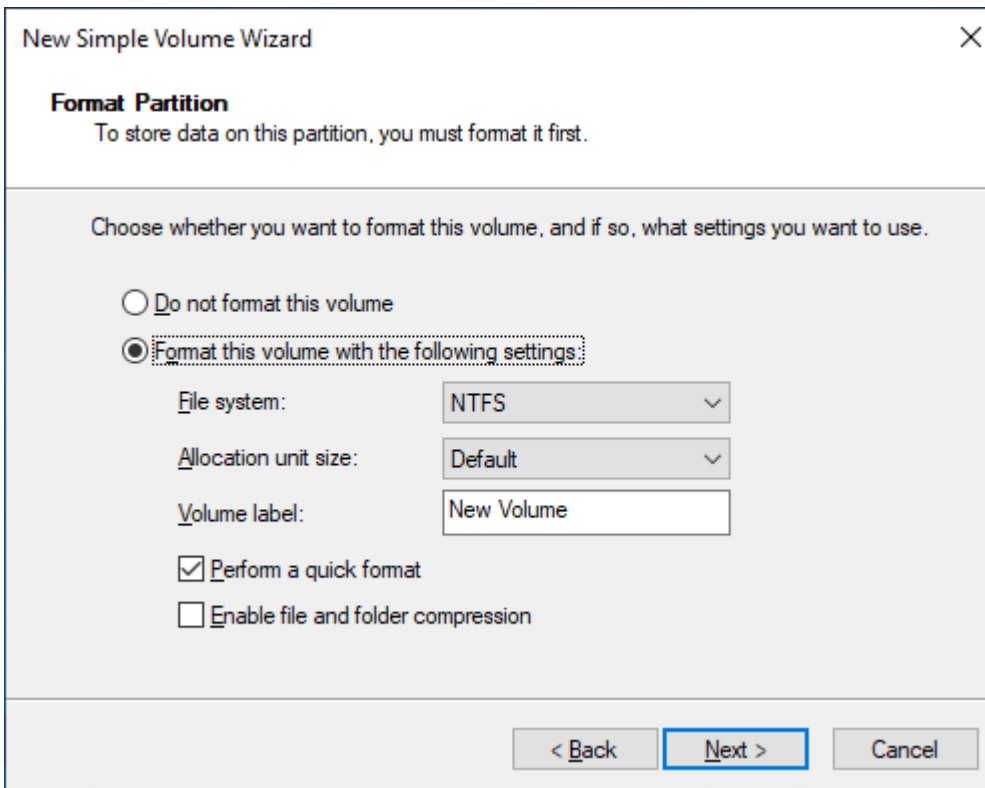
☒ Assign the following drive letter: D

☐ Mount in the following empty NTFS folder: Browse...

☐ Do not assign a drive letter or drive path

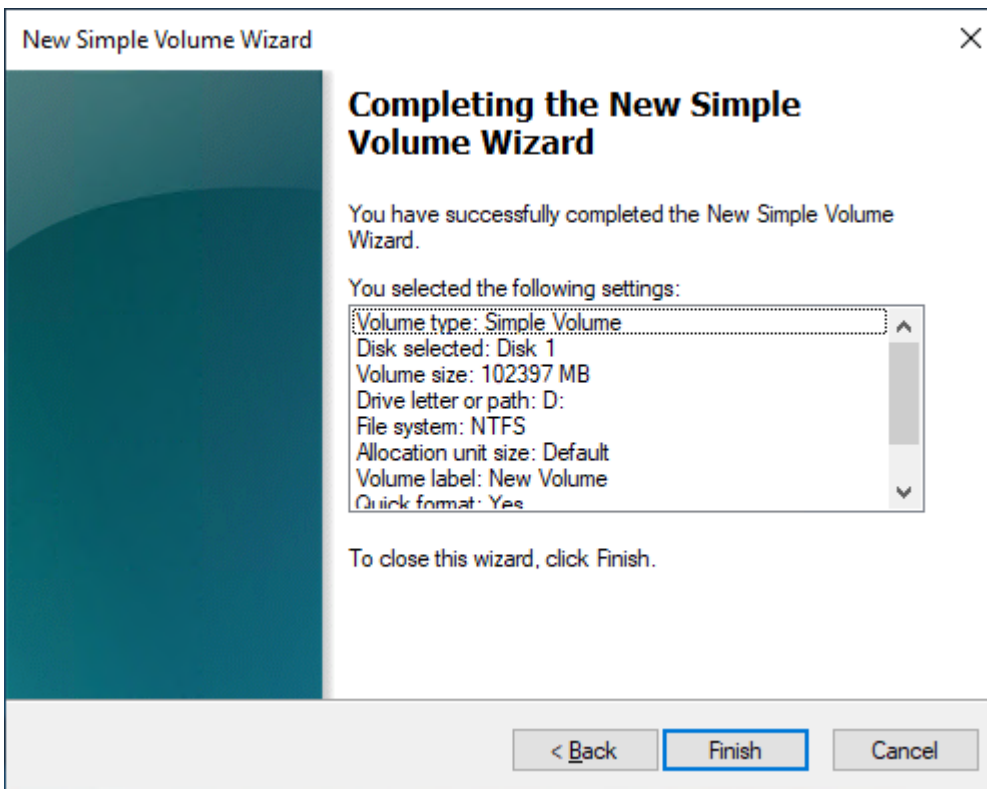
< Back Next > Cancel

9. Spécifiez une Étiquette du volume et réglez les paramètres par défaut, le cas échéant, puis choisissez Suivant.



The screenshot shows the 'New Simple Volume Wizard' dialog box, specifically the 'Format Partition' step. The title bar reads 'New Simple Volume Wizard' with a close button (X) on the right. Below the title, the section is titled 'Format Partition' with a subtitle 'To store data on this partition, you must format it first.' The main instruction says 'Choose whether you want to format this volume, and if so, what settings you want to use.' There are two radio button options: 'Do not format this volume' (unselected) and 'Format this volume with the following settings:' (selected). Under the selected option, there are three settings: 'File system:' set to 'NTFS' (dropdown), 'Allocation unit size:' set to 'Default' (dropdown), and 'Volume label:' set to 'New Volume' (text input). There are two checkboxes: 'Perform a quick format' (checked) and 'Enable file and folder compression' (unchecked). At the bottom, there are three buttons: '< Back' (disabled), 'Next >' (highlighted with a blue border), and 'Cancel' (disabled).

10. Vérifiez vos paramètres, puis choisissez Terminer pour appliquer les modifications et fermer l'Assistant Création d'un volume simple.



Afficher des informations sur un volume Amazon EBS

Vous pouvez visualiser les informations descriptives relatives à vos volumes EBS. Par exemple, vous pouvez consulter des informations sur tous les volumes d'une région spécifique ou consulter des informations détaillées sur un seul volume, notamment sa taille, son type de volume, si le volume est chiffré, quelle clé KMS a été utilisée pour chiffrer le volume et l'instance spécifique à laquelle le volume est attaché.

Vous pouvez obtenir des informations supplémentaires sur vos volumes EBS, telles que l'espace disque disponible, à partir du système d'exploitation sur l'instance.

Table des matières

- [Afficher des informations sur un volume](#)
- [États du volume](#)
- [Afficher les métriques de volume](#)
- [Afficher l'espace disque disponible](#)

Afficher des informations sur un volume

Vous pouvez consulter les informations relatives à vos volumes EBS.

Console

Pour afficher les informations relatives à un volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Pour réduire la liste, vous pouvez filtrer vos volumes à l'aide des identifications et des attributs de volume. Choisissez le champ de filtre, sélectionnez une identification ou un attribut de volume, puis sélectionnez la valeur du filtre.
4. Pour afficher des informations supplémentaires sur un volume, sélectionnez son ID.

Pour afficher les volumes EBS qui sont attachés à une instance

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Dans l'onglet Storage (Stockage), la section Block devices (Périphériques de bloc) répertorie les volumes attachés à l'instance. Pour afficher des informations sur un volume spécifique, choisissez son ID dans la colonne Volume ID (ID du volume).

Amazon EC2 Global View

Vous pouvez utiliser [Amazon EC2 Global View](#) pour consulter vos volumes dans toutes les régions pour lesquelles votre AWS compte est activé.

Pour obtenir un résumé de vos volumes EBS dans toutes les régions

1. Ouvrez la console Amazon EC2 Global View à <https://console.aws.amazon.com/ec2globalview/home> l'adresse.
2. Dans l'onglet Explorateur de régions, sous Résumé, vérifiez le nombre de ressources pour les volumes, qui inclut le nombre de volumes et le nombre de régions. Choisissez le texte souligné pour voir comment le nombre de volumes est réparti entre les régions.

3. Dans l'onglet Recherche globale, sélectionnez le filtre client Type de ressource = Volume. Vous pouvez filtrer davantage les résultats en spécifiant une région ou une balise.

AWS CLI

Pour afficher des informations sur un volume EBS

Utilisez la commande [describe-volumes](#). L'exemple suivant compte les volumes de la région actuelle.

```
aws ec2 describe-volumes --query "length(Volumes[*])"
```

L'exemple suivant répertorie les volumes attachés à l'instance spécifiée.

```
aws ec2 describe-volumes \
  --filters "Name=attachment.instance-id,Values=i-1234567890abcdef0" \
  --query Volumes[*].VolumeId \
  --output text
```

L'exemple suivant décrit le volume spécifié.

```
aws ec2 describe-volumes --volume-ids vol-01234567890abcdef
```

Voici un exemple de sortie.

```
{
  "Volumes": [
    {
      "Iops": 3000,
      "VolumeType": "gp3",
      "MultiAttachEnabled": false,
      "Throughput": 125,
      "Operator": {
        "Managed": false
      },
      "VolumeId": "vol-01234567890abcdef",
      "Size": 8,
      "SnapshotId": "snap-0abcdef1234567890",
      "AvailabilityZone": "us-west-2b",
      "State": "in-use",
    }
  ]
}
```

```

    "CreateTime": "2024-05-17T23:23:00.400000+00:00",
    "Attachments": [
      {
        "DeleteOnTermination": true,
        "VolumeId": "vol-01234567890abcdef",
        "InstanceId": "i-1234567890abcdef0",
        "Device": "/dev/xvda",
        "State": "attached",
        "AttachTime": "2024-05-17T23:23:00+00:00"
      }
    ],
    "Encrypted": false
  }
]
}

```

PowerShell

Pour afficher des informations sur un volume EBS

Utilisez l'applet de commande [Get-EC2Volume](#). L'exemple suivant compte les volumes de la région actuelle.

```
(Get-EC2Volume).Count
```

L'exemple suivant répertorie les volumes attachés à l'instance spécifiée.

```
(Get-EC2Volume `
  -Filters @{Name="attachment.instance-id";Values="i-1234567890abcdef0"}).VolumeId
```

L'exemple suivant décrit le volume spécifié.

```
Get-EC2Volume -VolumeId vol-01234567890abcdef
```

Voici un exemple de sortie.

```

Attachments      : {i-1234567890abcdef0}
AvailabilityZone  : us-west-2b
CreateTime       : 5/17/2024 11:23:00 PM
Encrypted        : False

```



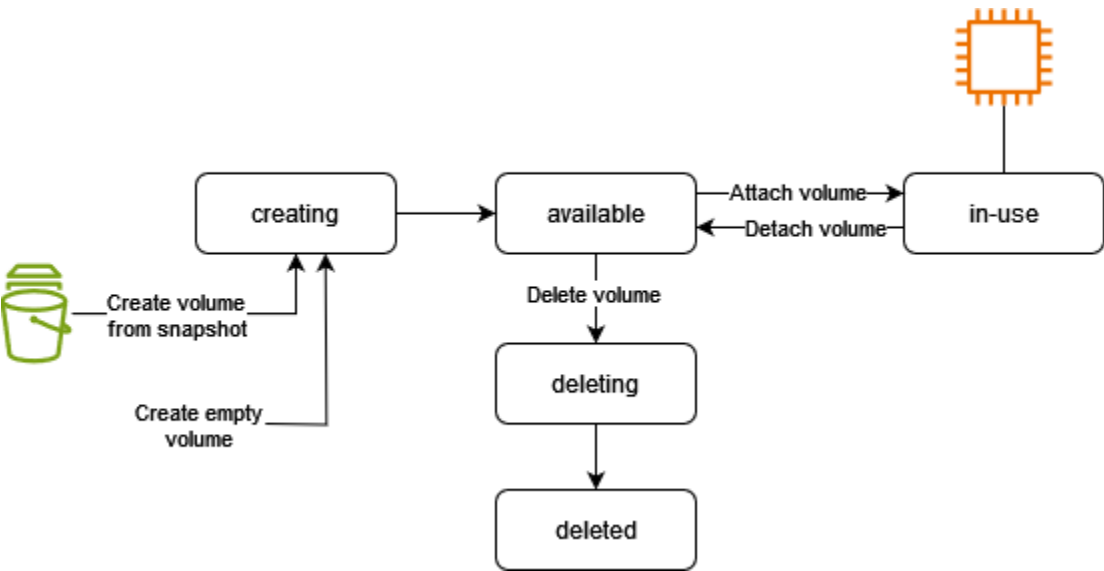
```
FastRestored      : False
Iops              : 3000
KmsKeyId          :
MultiAttachEnabled : False
Operator          : Amazon.EC2.Model.OperatorResponse
OutpostArn        :
Size              : 8
SnapshotId        : snap-0abcdef1234567890
SseType           :
State             : in-use
Tags              : {}
Throughput         : 125
VolumeId          : vol-01234567890abcdef
VolumeType        : gp3
```

États du volume

L'état du volume décrit la disponibilité d'un volume Amazon EBS. Vous pouvez consulter l'état du volume dans la colonne **État** de la page **Volumes** de la console ou à l'aide de la commande [describe-volumes](#) AWS CLI .

Un volume Amazon EBS passe par différents états entre le moment où il est créé et celui où il est supprimé.

L'illustration suivante montre les transitions entre les états de volume. Vous pouvez créer un volume à partir d'un instantané Amazon EBS ou créer un volume vide. Lorsque vous créez un volume, il entre dans **creating** cet état. Une fois que le volume est prêt à être utilisé, il entre dans l'**available** état. Vous pouvez associer un volume disponible à une instance située dans la même zone de disponibilité que le volume. Vous devez détacher le volume avant de pouvoir l'associer à une autre instance ou le supprimer. Vous pouvez supprimer un volume lorsque vous n'en avez plus besoin.



Le tableau suivant récapitule les états des volumes.

State	Description
creating	Le volume est en cours de création.
available	Le volume n'est pas attaché à une instance.
in-use	Le volume est attaché à une instance.
deleting	Le volume est en cours de suppression.
deleted	Le volume est supprimé.
error	Le matériel sous-jacent associé à votre volume EBS a échoué et les données associées au volume ne peuvent pas être récupérées. Pour plus d'informations sur la manière de restaurer le volume ou de récupérer les données qu'il contient, voir Pourquoi mon volume EBS a-t-il le statut « erreur » ? .

Afficher les métriques de volume

Vous pouvez obtenir des informations supplémentaires sur vos volumes EBS auprès d'Amazon CloudWatch. Pour plus d'informations, consultez [Statistiques CloudWatch Amazon pour Amazon EBS](#).

Afficher l'espace disque disponible

Vous pouvez obtenir des informations supplémentaires sur vos volumes EBS, telles que l'espace disque disponible, à partir du système d'exploitation sur l'instance.

Instances Linux

Utilisez la `df -hT` commande et spécifiez le nom de l'appareil :

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/xvda1      xfs       8.0G   1.2G   6.9G  15% /
```

instances Windows

Vous pouvez afficher l'espace disque disponible en ouvrant l'Explorateur de fichiers et en sélectionnant Ce PC.

Vous pouvez également afficher l'espace disque disponible en utilisant la commande `dir` suivante et en examinant la dernière ligne de la sortie :

```
C:\> dir C:
Volume in drive C has no label.
Volume Serial Number is 68C3-8081

Directory of C:\

03/25/2018  02:10 AM    <DIR>          .
03/25/2018  02:10 AM    <DIR>          ..
03/25/2018  03:47 AM    <DIR>          Contacts
03/25/2018  03:47 AM    <DIR>          Desktop
03/25/2018  03:47 AM    <DIR>          Documents
03/25/2018  03:47 AM    <DIR>          Downloads
03/25/2018  03:47 AM    <DIR>          Favorites
03/25/2018  03:47 AM    <DIR>          Links
03/25/2018  03:47 AM    <DIR>          Music
03/25/2018  03:47 AM    <DIR>          Pictures
03/25/2018  03:47 AM    <DIR>          Saved Games
03/25/2018  03:47 AM    <DIR>          Searches
03/25/2018  03:47 AM    <DIR>          Videos
                0 File(s)                0 bytes
               13 Dir(s)  18,113,662,976 bytes free
```

Vous pouvez également afficher l'espace disque disponible en utilisant la commande `fsutil` suivante :

```
C:\> fsutil volume diskfree C:
Total # of free bytes      : 18113204224
Total # of bytes          : 32210153472
Total # of avail free bytes : 18113204224
```

Tip

Vous pouvez également utiliser l' CloudWatch agent pour collecter des mesures d'utilisation de l'espace disque à partir d'une instance Amazon EC2 sans vous connecter à l'instance. Pour plus d'informations, consultez [Création du fichier de configuration de l' CloudWatch agent](#) et [Installation de l' CloudWatch agent](#) dans le Guide de CloudWatch l'utilisateur Amazon. Si vous devez surveiller l'utilisation de l'espace disque pour plusieurs instances, vous pouvez installer et configurer l' CloudWatch agent sur ces instances à l'aide de Systems Manager. Pour plus d'informations, consultez la section [Installation de l' CloudWatch agent à l'aide de Systems Manager](#).

Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes

Amazon EBS Elastic Volumes vous permet d'augmenter la taille du volume, de changer le type de volume ou d'ajuster les performances de vos volumes EBS. Si votre instance prend en charge Elastic Volumes, vous pouvez procéder sans détacher le volume ni redémarrer l'instance. Cela vous permet de continuer à utiliser votre application pendant que les modifications prennent effet.

Aucuns frais supplémentaires ne sont facturés pour modifier la configuration d'un volume. La configuration du nouveau volume vous est facturée une fois que la modification du volume a commencé. Pour plus d'informations, consultez la page [Tarification d'Amazon EBS](#).

Table des matières

- [Considérations](#)
- [Limitations](#)
- [Exigences relatives aux modifications des volumes Amazon EBS](#)
- [Demander des modifications de volume Amazon EBS](#)
- [Surveillez la progression des modifications des volumes Amazon EBS](#)

- [Étendre le système de fichiers après avoir redimensionné un volume Amazon EBS](#)

Considérations

- Après avoir initié une modification de volume, vous devez attendre que cette modification atteigne l'état voulu avant de pouvoir lancer une autre modification pour le même volume. Vous pouvez modifier un volume jusqu'à quatre fois sur une période continue de 24 heures, à condition que le volume soit à l'état `available` ou `in-use` et que toutes les modifications précédentes apportées à ce volume le soient. Si vous dépassez cette limite, un message d'erreur vous indique quand vous pouvez effectuer votre prochaine modification.
- Les modifications de volume sont effectuées dans la mesure du possible et leur exécution peut prendre de quelques minutes à quelques heures, selon la configuration de volume demandée. En règle générale, la modification d'un volume de 1 TiB peut prendre jusqu'à six heures. Cependant, le temps ne varie pas toujours de manière linéaire avec la taille du volume : un volume plus important peut prendre moins de temps, et un volume plus petit peut prendre plus de temps.
- Les augmentations de taille prennent effet une fois que la modification du volume atteint l'état `optimizing`, ce qui prend généralement quelques secondes.
- La durée de modification est augmentée pour les volumes qui ne sont pas entièrement initialisés. Pour plus d'informations, consultez [Initialiser manuellement les volumes après leur création](#).
- Si vous modifiez le type de volume de `gp2` à `gp3` sans spécifier les performances d'IOPS ou de débit, Amazon EBS provisionne automatiquement les performances. Il utilise soit les performances équivalentes du `gp2` volume source, soit les `gp3` performances de référence, la valeur la plus élevée étant retenue.

Par exemple, si vous modifiez un `gp2` volume de 500 GiB avec un MiB/s débit de 250 et 1 500 IOPS `gp3` sans spécifier les performances d'IOPS ou de débit, Amazon EBS provisionne automatiquement le `gp3` volume avec 3 000 IOPS (IOPS de base `gp3`) et 250 MiB/s (pour correspondre au débit du volume source).

- Si vous recevez un message d'erreur lorsque vous tentez de modifier un volume EBS ou que vous êtes sur le point de modifier un volume EBS attaché à un type d'instance de la génération précédente, effectuez l'une des actions suivantes :
 - Pour un volume non-racine, détachez le volume de l'instance, appliquez les modifications, puis attachez à nouveau le volume.
 - Pour un volume racine, arrêtez l'instance, appliquez les modifications, puis redémarrez l'instance.

Limitations

- Vous ne pouvez pas annuler une demande de modification de volume une fois qu'elle a été envoyée.
- Vous devez augmenter la taille du volume. Vous ne pouvez pas diminuer la taille du volume. Vous pouvez toutefois créer un volume plus petit, puis y migrer vos données à l'aide d'un outil au niveau de l'application tel que rsync (instances Linux) ou robocopy (instances Windows).
- Il existe des limites au stockage agrégé maximal qui peut être demandé pour les modifications de volume. Pour plus d'informations, consultez [Quotas du service Amazon EBS](#) dans le Référence générale d'Amazon Web Services.
- La nouvelle taille de volume ne peut pas dépasser la capacité prise en charge de son système de fichiers et de son schéma de partitionnement. Pour plus d'informations, consultez [Contraintes de volume Amazon EBS](#).
- Si vous ne modifiez pas le type de volume, les modifications de taille et de performances du volume doivent s'inscrire dans les limites du type de volume actuel. Si vous modifiez le type de volume, les modifications de taille et de performances du volume doivent s'inscrire dans les limites du type de volume cible. Pour plus d'informations, consultez [Types de volume Amazon EBS](#).
- [Nitro-based les instances](#) prennent en charge des volumes provisionnés avec un maximum de 256 000 IOPS. D'autres types d'instances peuvent être connectés à des volumes alloués avec jusqu'à 64 000 IOPS, mais peuvent atteindre 32 000 IOPS.
- Pour les volumes Multi-Attach activés, vous pouvez modifier le type de volume dans les deux sens io1 et io2 dans les deux sens, y compris lorsque le volume est connecté. Les autres modifications de type de volume ne sont pas prises en charge.

Lorsque vous modifiez le type de volume entre io1 et io2 pour un volume Multi-Attach activé, l'état d'activation des réservations NVMe du volume est transféré au type de volume cible.

- Un volume racine de type io1, io2, gp2, gp3, ou standard ne peut pas être modifié en volume st1 ou sc1, même s'il est détaché de l'instance.
- Si le volume a été attaché avant le 3 novembre 2016 à 23 h 40 UTC, vous devez initialiser la prise en charge d'Elastic Volumes. Pour plus d'informations, consultez [Initialisation de la prise en charge d'Elastic Volumes](#).
- Alors que les instances m3.medium prennent pleinement en charge la modification du volume, m3.large, m3.xlarge, et m3.2xlarge peuvent ne pas prendre en charge toutes les fonctionnalités de modification de volume.

Exigences relatives aux modifications des volumes Amazon EBS

Les exigences et les limites suivantes s'appliquent lorsque vous modifiez un volume Amazon EBS. Pour en savoir plus sur les exigences générales des volumes EBS, consultez [Contraintes de volume Amazon EBS](#).

Rubriques

- [Types d'instance pris en charge](#)
- [Système d'exploitation](#)

Types d'instance pris en charge

Elastic Volumes est pris en charge sur les instances suivantes :

- Toutes les instances de la génération [actuelle](#)
- Les instances de génération précédente suivantes : C1, C3, C4, G2, I2, M1, M3, M4, R3, and R4

Si votre type d'instance ne prend pas en charge Elastic Volumes, consultez [Modifier un volume EBS si Elastic Volumes n'est pas pris en charge](#).

Système d'exploitation

Les exigences de système d'exploitation suivantes s'appliquent :

Linux

Les AMI Linux exigent une table de partition GPT GUID et GRUB 2 pour les volumes de démarrage de 2 Tio (2 048 Gio) ou plus. Beaucoup d'AMI Linux utilisent encore le schéma de partitionnement MBR, qui prend en charge seulement les volumes de démarrage de 2 Tio maximum. Si votre instance ne démarre pas avec un volume de démarrage supérieur à 2 TiB, l'AMI que vous utilisez peut être limitée à un volume de démarrage inférieur à 2 TiB. Non-boot les volumes ne sont pas soumis à cette limitation sur les instances Linux.

Avant de redimensionner un volume de démarrage avec une capacité de plus de 2 Tio, vous pouvez déterminer si le volume utilise un partitionnement MBR ou GPT en exécutant la commande suivante sur votre instance :

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

Une instance Amazon Linux avec un partitionnement GPT renvoie les informations suivantes :

```
GPT fdisk (gdisk) version 0.8.10
```

```
Partition table scan:
```

```
MBR: protective  
BSD: not present  
APM: not present  
GPT: present
```

```
Found valid GPT with protective MBR; using GPT.
```

Une instance SUSE avec un partitionnement MBR renvoie les informations suivantes :

```
GPT fdisk (gdisk) version 0.8.8
```

```
Partition table scan:
```

```
MBR: MBR only  
BSD: not present  
APM: not present  
GPT: not present
```

Windows

Par défaut, Windows initialise les volumes avec une table de partition MBR (Master Boot Record). Comme MBR prend uniquement en charge les volumes dont la taille est inférieure à 2 To (2 048 Go), Windows vous empêche de redimensionner les volumes MBR au-delà de cette limite. Dans ce cas, l'option Extend Volume (Étendre le volume) est désactivée dans l'utilitaire Windows Gestion des disques. Si vous utilisez le Console de gestion AWS ou AWS CLI pour créer un MBR-partitioned volume qui dépasse la limite de taille, Windows ne peut pas détecter ni utiliser l'espace supplémentaire.

Pour contourner cette limite, vous pouvez créer un nouveau volume plus grand avec une table de partition GUID (GPT) et y copier les données du volume MBR d'origine.

Pour créer un volume GPT

1. Créez un nouveau volume vide de la taille souhaitée dans la zone de disponibilité de l'instance EC2 et attachez-le à votre instance.

 Note

Le nouveau volume ne doit pas être un volume restauré à partir d'un instantané.

2. Connectez-vous au système Windows et ouvrez Gestion des disques (diskmgmt.exe).
3. Ouvrez le menu contextuel (clic droit) pour le disque et choisissez En ligne.
4. Dans la fenêtre Initialiser le disque, sélectionnez le nouveau disque et choisissez Partition GPT (GUID Partition Table), puis OK.
5. Lorsque l'initialisation est terminée, copiez les données du volume d'origine vers le nouveau volume à l'aide d'un outil comme robocopy ou teracopy.
6. Dans Gestion des disques, modifiez les lettres des lecteurs avec les valeurs correspondantes et déconnectez l'ancien volume.
7. Dans la console Amazon EC2, détachez l'ancien volume de l'instance, redémarrez l'instance pour vérifier qu'elle fonctionne correctement, puis supprimez l'ancien volume.

Demander des modifications de volume Amazon EBS

Avec Elastic Volumes, vous pouvez augmenter de manière dynamique la taille, les performances et le type de vos volumes Amazon EBS sans les détacher.

Présentation du processus

1. (Facultatif) Avant de modifier un volume contenant des données importantes, une bonne pratique consiste à créer un instantané du volume au cas où vous auriez besoin d'annuler vos modifications. Pour plus d'informations, consultez [Créer des instantanés Amazon EBS](#).
2. Demandez la modification du volume.
3. Surveillez la progression de la modification du volume. Pour plus d'informations, consultez [Surveillez la progression des modifications des volumes Amazon EBS](#).
4. Si la taille du volume a été modifiée, étendez le système de fichiers du volume pour tirer parti de la capacité de stockage accrue. Pour plus d'informations, consultez [Étendre le système de fichiers après avoir redimensionné un volume Amazon EBS](#).

Sommaire

- [Modifier un volume EBS à l'aide d'Elastic Volumes](#)

- [Modifier un volume EBS si Elastic Volumes n'est pas pris en charge](#)
- [Initialiser la prise en charge d'Elastic Volumes \(si nécessaire\)](#)

Modifier un volume EBS à l'aide d'Elastic Volumes

Avant de commencer, consultez les points suivants :

- [Considérations](#)
- [Limites](#)
- [Exigences](#)

Console

Pour modifier un volume EBS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume, puis Actions et Modify volume (Modifier un volume).
4. La fenêtre Modify volume (Modifier un volume) affiche l'ID du volume et la configuration actuelle du volume, notamment le type, la taille, les IOPS et le débit. Définissez les nouvelles valeurs de configuration comme suit :
 - Afin de modifier le type, choisissez une valeur pour Volume type (Type de volume).
 - Pour modifier la taille, saisissez une nouvelle valeur pour Taille.
 - (gp3, io1 et io2 seulement) Afin de modifier les IOPS, saisissez une nouvelle valeur pour les IOPS.
 - (gp3 seulement) Afin de modifier le débit, saisissez une nouvelle valeur pour Throughput (Débit).
5. Une fois que vous avez fini de modifier les paramètres du volume, choisissez Modifier. Lorsque vous êtes invité à confirmer l'opération, choisissez Modify (Modifier).
6. Si vous avez augmenté la taille de votre volume, vous devez également étendre la partition du volume pour utiliser la capacité de stockage supplémentaire. Pour plus d'informations, consultez [Étendre le système de fichiers après avoir redimensionné un volume Amazon EBS](#).
7. (Instances Windows uniquement) Si vous augmentez la taille d'un volume NVMe sur une instance qui ne possède pas les pilotes AWS NVMe, vous devez redémarrer l'instance

pour permettre à Windows de voir la nouvelle taille de volume. Pour plus d'informations sur l'installation des pilotes AWS NVMe, consultez la section Pilotes [AWS NVMe](#).

AWS CLI

Pour modifier un volume EBS

Utilisez la commande [modify-volume](#). Par exemple, si vous disposez d'un volume de type gp2 d'une taille de 100 GiB, l'exemple suivant change sa configuration en un volume de type io1 avec 10 000 IOPS et une taille de 200 GiB.

```
aws ec2 modify-volume \  
  --volume-id vol-01234567890abcdef \  
  --volume-type io1 \  
  --iops 10000 \  
  --size 200
```

Voici un exemple de sortie.

```
{  
  "VolumeModification": {  
    "TargetSize": 200,  
    "TargetVolumeType": "io1",  
    "ModificationState": "modifying",  
    "VolumeId": "vol-01234567890abcdef",  
    "TargetIops": 10000,  
    "StartTime": "2022-01-19T22:21:02.959Z",  
    "Progress": 0,  
    "OriginalVolumeType": "gp2",  
    "OriginalIops": 300,  
    "OriginalSize": 100  
  }  
}
```

Si vous avez augmenté la taille de votre volume, vous devez également étendre la partition du volume pour utiliser la capacité de stockage supplémentaire. Pour plus d'informations, consultez [Étendre le système de fichiers après avoir redimensionné un volume Amazon EBS](#).

PowerShell

Pour modifier un volume EBS

Utilisez l'applet de commande [Edit-EC2Volume](#). Par exemple, si vous disposez d'un volume de type gp2 d'une taille de 100 GiB, l'exemple suivant change sa configuration en un volume de type io1 avec 10 000 IOPS et une taille de 200 GiB.

```
Edit-EC2Volume `
  -VolumeId vol-01234567890abcdef `
  -VolumeType io1 `
  -Iops 10000 `
  -Size 200
```

Si vous avez augmenté la taille de votre volume, vous devez également étendre la partition du volume pour utiliser la capacité de stockage supplémentaire. Pour plus d'informations, consultez [Étendre le système de fichiers après avoir redimensionné un volume Amazon EBS](#).

Modifier un volume EBS si Elastic Volumes n'est pas pris en charge

Si vous utilisez un type d'instance pris en charge, vous pouvez utiliser Elastic Volumes pour modifier dynamiquement la taille, les performances et le type de volume de vos volumes Amazon EBS sans les détacher.

Si vous ne pouvez pas utiliser Elastic Volumes mais que vous devez modifier le volume racine (de démarrage), vous devez arrêter l'instance, modifier le volume, puis redémarrer l'instance.

Une fois que l'instance a démarré, vous pouvez vérifier la taille du système de fichiers pour vérifier que votre instance reconnaît l'espace de volume agrandi. Sur Linux, utilisez la commande `df -h` pour vérifier la taille du système de fichiers.

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       7.9G  943M   6.9G  12% /
tmpfs           1.9G     0   1.9G   0% /dev/shm
```

Si la taille ne reflète pas votre volume nouvellement étendu, vous devez étendre le système de fichiers de votre périphérique pour permettre à votre instance d'utiliser le nouvel espace. Pour plus d'informations, consultez [Étendre le système de fichiers après avoir redimensionné un volume Amazon EBS](#).

Dans le cas des instances Windows, il se peut que vous deviez mettre le volume en ligne pour pouvoir l'utiliser. Pour plus d'informations, consultez [Mettre un volume Amazon EBS à disposition pour utilisation](#). Vous n'avez pas besoin de reformater le volume.

Initialiser la prise en charge d'Elastic Volumes (si nécessaire)

Avant de pouvoir modifier un volume attaché à une instance avant le 3 novembre 2016 à 23 h 40 UTC, vous devez initialiser la prise en charge de modification des volumes par l'une des actions suivantes :

- Détacher et attacher le volume
- Arrêter et démarrer l'instance

Console

Pour déterminer si vos instances sont prêtes

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances.
3. Choisissez l'icône Show/Hide Colonnes (l'engrenage). Sélectionnez la colonne d'attribut Heure de lancement, puis choisissez Confirmer.
4. Triez la liste d'instances par colonne d'Heure de lancement. Pour chaque instance démarrée avant la date limite, choisissez l'onglet Stockage et cochez la colonne Heure des pièces jointes pour voir quand ses volumes ont été attachés.

AWS CLI

Pour déterminer si vos instances sont prêtes

Utilisez la commande [describe-instances](#) suivante pour déterminer si le volume a été attaché avant le 3 novembre 2016 à 23 h 40 UTC.

```
aws ec2 describe-instances \
  --query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" \
  --output text
```

Pour chaque instance, la première ligne de la sortie montre son ID et si elle a été démarrée avant la date de coupure (vrai ou faux). La première ligne est suivie d'une ou plusieurs lignes qui montrent si chaque volume EBS a été attaché avant la date de coupure (vrai ou faux). Dans la sortie de l'exemple suivant, vous devez initialiser la modification des volumes pour la première

instance car elle a commencé avant la date de coupure et son volume de racine a été attaché avant la date de coupure. Les autres instances sont prêtes car elles ont été démarrées après la date de coupure.

```
i-e905622e      True
True
i-719f99a8      False
True
i-006b02c1b78381e57  False
False
False
i-e3d172ed      False
True
```

PowerShell

Pour déterminer si une instance est prête

Utilisez l'[Get-EC2Instance](#) applet de commande pour déterminer si un volume a été attaché avant le 3 novembre 2016 à 23h40 UTC.

```
(Get-EC2Instance `
  -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings | `
  Format-Table @{"Name"="VolumeId";Expression={$_.Ebs.VolumeId}}, `
               @{"Name"="AttachTime";Expression={$_.Ebs.AttachTime}}
```

Voici un exemple de sortie.

```
VolumeId      AttachTime
-----
vol-0b243c8d927752d2b 3/23/2020 12:21:14 AM
vol-043eadbeb4a8387c3 9/5/2020 7:39:22 PM
vol-0c3f0c4e55c082753 4/23/2019 4:07:40 PM
```

Surveillez la progression des modifications des volumes Amazon EBS

Lorsque vous modifiez un volume EBS, il passe par une suite d'états. Le volume passe à l'état `modifying`, à l'état `optimizing` et enfin à l'état `completed`. A ce stade, le volume est prêt à recevoir d'autres modifications.

Lorsque le volume a l'état `optimizing`, ses performances se situent entre les spécifications de configuration source et les spécifications de configuration cible. Les performances de volume transitoires ne seront jamais inférieures aux performances de volume source. Si vous mettez à niveau les opérations d'IOPS, les performances de volume transitoires ne seront jamais inférieures aux performances de volume cible.

Les changements des modifications du volume prennent effet comme suit :

- Les augmentations de taille prennent effet une fois que la modification du volume atteint `optimizing` l'état, ce qui prend généralement quelques secondes.
- Les modifications de performances (IOPS et débit) peuvent prendre de quelques minutes à quelques heures, selon la configuration de volume demandée. En règle générale, la migration d'un volume de 1 TiB entièrement utilisé vers une nouvelle configuration de performances peut prendre environ 6 heures. Dans certains cas, l'entrée en vigueur d'une nouvelle configuration de performances peut prendre plus de 24 heures, par exemple lorsque le volume n'a pas été complètement initialisé.

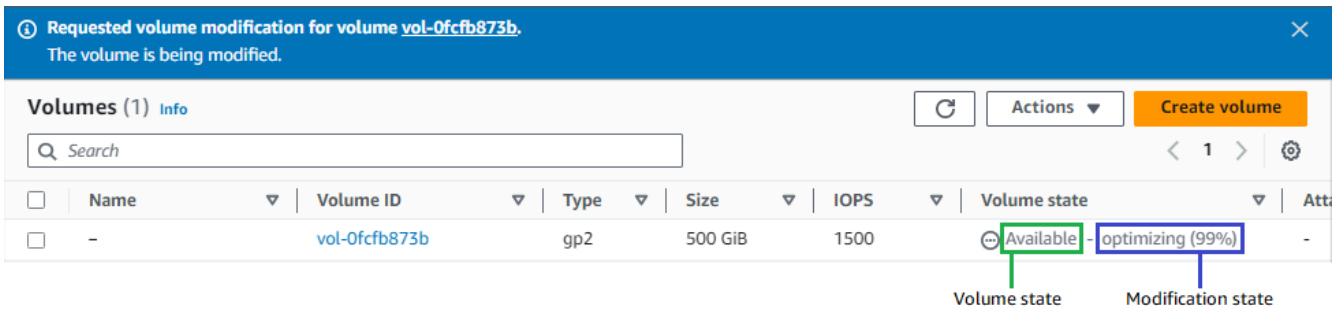
Les états de volume possibles sont les suivants : `creating`, `available`, `in-use`, `deleting`, `deleted` et `error`.

Les états de modification possibles sont `modifying`, `optimizing` et `completed`.

Console

Pour suivre la progression d'une modification

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume.
4. La colonne État du volume et le champ État du volume de l'onglet Détails contiennent des informations au format suivant : *Volume state - Modification state (Modification progress%)*. L'image suivante montre le volume et les états de modification du volume.



Une fois la modification terminée, seul l'état du volume est affiché. L'état de modification et la progression ne sont plus affichés.

Vous pouvez également utiliser Amazon EventBridge pour créer une règle de notification pour les événements de modification de volume. Pour plus d'informations, consultez la section [Premiers pas avec Amazon EventBridge](#).

AWS CLI

Pour suivre la progression d'une modification

Utilisez la commande [describe-volumes-modifications](#) pour afficher la progression d'une ou de plusieurs modifications d'un volume. L'exemple suivant décrit les modifications de volume de deux volumes.

```
aws ec2 describe-volumes-modifications \
  --volume-ids vol-11111111111111111 vol-22222222222222222
```

Dans l'exemple de sortie suivant, les modifications de volume sont encore à l'état `modifying`. La progression est présentée en pourcentage.

```
{
  "VolumesModifications": [
    {
      "TargetSize": 200,
      "TargetVolumeType": "io1",
      "ModificationState": "modifying",
      "VolumeId": "vol-11111111111111111",
      "TargetIops": 10000,
      "StartTime": "2017-01-19T22:21:02.959Z",
      "Progress": 0,
      "OriginalVolumeType": "gp2",
```



```

        "OriginalIops": 300,
        "OriginalSize": 100
    },
    {
        "TargetSize": 2000,
        "TargetVolumeType": "sc1",
        "ModificationState": "modifying",
        "VolumeId": "vol-2222222222222222",
        "StartTime": "2017-01-19T22:23:22.158Z",
        "Progress": 0,
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 1000
    }
]
}

```

L'exemple suivant décrit tous les volumes dont l'état de modification est `optimizing` ou `completed`, puis filtre et formate les résultats pour n'afficher que les modifications initiées le 1er février 2017 ou après cette date :

```

aws ec2 describe-volumes-modifications \
  --filters Name=modification-state,Values="optimizing","completed" \
  --query "VolumesModifications[?StartTime>='2017-02-01']".
{ID:VolumeId,STATE:ModificationState}"

```

Voici un exemple de sortie avec des informations sur deux volumes :

```

[
  {
    "STATE": "optimizing",
    "ID": "vol-06397e7a0eEXAMPLE"
  },
  {
    "STATE": "completed",
    "ID": "vol-ba74e18c2aEXAMPLE"
  }
]

```

PowerShell

Pour suivre la progression d'une modification

Utilisez l'applet de commande [Get-EC2VolumeModification](#). L'exemple suivant décrit les modifications de volume de deux volumes.

```
Get-EC2VolumeModification `
  -VolumeId vol-111111111111111111 vol-222222222222222222
```

Note

Dans de rares cas, un AWS défaut transitoire peut provoquer un failed état. Ceci n'indique pas la santé du volume, mais uniquement l'échec de modification du volume. Si cela se produit, réessayez de modifier le volume.

Étendre le système de fichiers après avoir redimensionné un volume Amazon EBS

Après avoir [augmenté la taille d'un volume EBS](#), vous devez étendre la partition et le système de fichiers à la nouvelle taille supérieure. Vous pouvez le faire dès que le volume entre dans l'état optimizing.

Avant de commencer

- Créez un instantané du volume, au cas où vous auriez besoin d'annuler vos modifications. Pour plus d'informations, consultez [Créer des instantanés Amazon EBS](#).
- Confirmez que la modification du volume a réussi et qu'il est dans l'état optimizing ou completed. Pour plus d'informations, consultez [Surveillez la progression des modifications des volumes Amazon EBS](#).
- Assurez-vous que le volume est attaché à l'instance, qu'il est formaté et monté. Pour plus d'informations, consultez [Formatage et montage d'un volume attaché](#).
- (Instances Linux uniquement) Si vous utilisez des volumes logiques sur le volume Amazon EBS, vous devez utiliser Logical Volume Manager (LVM) pour étendre le volume logique. Pour savoir comment procéder, consultez la section Étendre le LV de l'article [Comment utiliser LVM pour créer un volume logique sur la partition d'un volume EBS ?](#).

Instances Linux

Note

Les instructions suivantes vous guident tout au long du processus d'extension des systèmes de fichiers XFS et Ext4 pour Linux. Pour plus d'informations sur l'extension d'un autre système de fichiers, consultez sa documentation.

Avant de pouvoir étendre un système de fichiers sous Linux, vous devez étendre la partition, si votre volume en possède une.

Étendre le système de fichiers des volumes EBS

Utilisez la procédure suivante pour étendre le système de fichiers d'un volume redimensionné.

Notez que la dénomination des périphériques et des partitions diffère pour les instances Xen et les instances créées sur le système Nitro. Pour déterminer si votre instance est Xen-based ou Nitro-based, consultez la section Type d'hyperviseur [Amazon EC2](#).

Pour étendre le système de fichiers des volumes EBS

1. [Connectez-vous à votre instance](#).
2. Redimensionnez la partition, si nécessaire. Pour ce faire :
 - a. Vérifiez si le volume possède une partition. Utilisez la commande `lsblk`.

Nitro instance example

Dans l'exemple de sortie suivant, le volume racine (`nvme0n1`) possède deux partitions (`nvme0n1p1` et `nvme0n1p128`), tandis que le volume supplémentaire (`nvme1n1`) ne possède aucune partition.

```
[ec2-user ~]$ sudo lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1              259:0    0   30G  0 disk /data
nvme0n1              259:1    0   16G  0 disk
##nvme0n1p1         259:2    0    8G  0 part /
##nvme0n1p128       259:3    0    1M  0 part
```

Xen instance example

Dans l'exemple de sortie suivant, le volume racine (xvda) possède une partition (xvda1), tandis que le volume supplémentaire (xvdf) ne possède aucune partition.

```
[ec2-user ~]$ sudo lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda         202:0    0   16G  0 disk
##xvda1      202:1    0    8G  0 part /
xvdf         202:80   0   24G  0 disk
```

- Si le volume comporte une partition, passez à l'étape suivante (2b).
- Si le volume ne comporte aucune partition, ignorez les étapes 2b, 2c et 2d et passez à l'étape 3.

Conseil pour la résolution de problèmes

Si le volume n'apparaît pas dans la sortie de commande, assurez-vous qu'il est [attaché à l'instance](#), qu'il est [formaté et monté](#).

- b. Vérifiez si la partition doit être étendue. Dans la sortie de la commande `lsblk` de l'étape précédente, comparez la taille de la partition et celle du volume.
- Si la taille de la partition est inférieure à la taille du volume, passez à l'étape suivante (2c).
 - Si la taille de la partition est égale à la taille du volume, il n'est pas nécessaire de l'étendre. Ignorez les étapes 2c et 2d, puis passez à l'étape 3.

Conseil pour la résolution de problèmes

Si le volume reflète toujours la taille d'origine, [confirmez que la modification du volume a réussi](#).

- c. Étendez la partition. Utilisez la `growpart` commande et spécifiez le nom du périphérique et le numéro de partition.

Nitro instance example

Le numéro de partition est le numéro qui suit le p. Par exemple, pour `nvme0n1p1`, le numéro de partition est `1`. Pour `nvme0n1p128`, le numéro de partition est `128`.

Pour étendre une partition nommée `nvme0n1p1`, utilisez la commande suivante.



Important

Notez l'espace entre le nom du périphérique (`nvme0n1`) et le numéro de la partition (`1`).

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

Xen instance example

Le numéro de partition est le numéro qui suit le nom du périphérique. Par exemple, pour `xvda1`, le numéro de partition est `1`. Pour `xvda128`, le numéro de partition est `128`.

Pour étendre une partition nommée `xvda1`, utilisez la commande suivante.



Important

Notez l'espace entre le nom du périphérique (`xvda`) et le numéro de la partition (`1`).

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
```



Conseils pour le dépannage

- `mkdir: cannot create directory '/tmp/growpart.31171': No space left on device FAILED: failed to make temp dir:` indique qu'il n'y a pas assez d'espace disque libre sur le volume pour que

growpart puisse créer le répertoire temporaire dont il a besoin pour effectuer le redimensionnement. Libérez de l'espace disque, puis recommencez.

- `must supply partition-number` : indique que vous avez spécifié une partition incorrecte. Utilisez la `lsblk` commande pour confirmer le nom de la partition et assurez-vous de saisir un espace entre le nom du périphérique et le numéro de partition.
- `NOCHANGE: partition 1 is size 16773087. it cannot be grown` : indique que la partition couvre déjà la totalité du volume et ne peut pas être étendue. [Confirmez que la modification du volume a réussi.](#)

- Vérifiez que la partition a été étendue. Utilisez la commande `lsblk`. La taille de la partition devrait maintenant être égale à celle du volume.

Nitro instance example

L'exemple de sortie suivant montre que le volume (`nvme0n1`) et la partition (`nvme0n1p1`) ont la même taille (16 GB).

```
[ec2-user ~]$ sudo lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1             259:0    0   30G  0 disk /data
nvme0n1             259:1    0   16G  0 disk
##nvme0n1p1        259:2    0   16G  0 part /
##nvme0n1p128     259:3    0    1M  0 part
```

Xen instance example

L'exemple de sortie suivant montre que le volume (`xvda`) et la partition (`xvda1`) ont la même taille (16 GB).

```
[ec2-user ~]$ sudo lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda      202:0    0   16G  0 disk
##xvda1   202:1    0   16G  0 part /
xvdf      202:80   0   24G  0 disk
```

3. Étendre le système de fichiers.

- Obtenez le nom, la taille, le type et le point de montage du système de fichiers que vous devez étendre. Utilisez la `lsblk -f` commande `df -hT` ou.

Nitro instance example

L'exemple de sortie suivant pour la `df -hT` commande montre que le système de `/dev/nvme0n1p1` fichiers a une taille de 8 Go, que son type est `xfs` et que son point de montage est `/`.

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
/dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
...
```

Xen instance example

L'exemple de sortie suivant pour la `df -hT` commande montre que le système de `/dev/xvda1` fichiers a une taille de 8 Go, que son type est `ext4` et que son point de montage est `/`.

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used  Avail  Use%  Mounted on
/dev/xvda1      ext4  8.0G  1.9G  6.2G   24%  /
/dev/xvdf1      xfs   24.0G  45M  8.0G   1%  /data
...
```

- Si la taille du système de fichiers est inférieure à la taille du volume, passez à l'étape suivante (3b).
 - Si la taille du système de fichiers est égale à la taille du volume, il n'est pas nécessaire de l'étendre. Dans ce cas, ignorez les étapes restantes : la partition et le système de fichiers ont été étendus à la nouvelle taille de volume.
- b. Les commandes permettant d'étendre le système de fichiers diffèrent en fonction du type de système de fichiers. Choisissez la commande correcte suivante en fonction du type de système de fichiers que vous avez noté à l'étape précédente.
- [Système de fichiers XFS] Utilisez la commande `xfs_growfs` et spécifiez le point de montage du système de fichiers que vous avez noté à l'étape précédente.

Nitro and Xen instance example

Par exemple, pour étendre un système de fichiers monté sur /, utilisez la commande suivante.

```
[ec2-user ~]$ sudo xfs_growfs -d /
```

Conseils pour le dépannage

- `xfs_growfs: /data is not a mounted XFS filesystem` : indique que vous avez spécifié un point de montage incorrect ou que le système de fichiers n'est pas XFS. Pour vérifier le point de montage et le type de système de fichiers, utilisez la commande `df -hT`.
 - `data size unchanged, skipping` : indique que le système de fichiers occupe déjà l'ensemble du volume. Si le volume ne comporte pas de partitions, [confirmez que la modification du volume a réussi](#). Si le volume comporte des partitions, assurez-vous que la partition a été étendue comme décrit à l'étape 2.
- [Système de fichiers Ext4] Utilisez la commande `resize2fs` et spécifiez le nom du système de fichiers que vous avez noté à l'étape précédente.

Nitro instance example

Par exemple, pour étendre un système de fichiers monté nommé `/dev/nvme0n1p1`, utilisez la commande suivante.

```
[ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
```

Xen instance example

Par exemple, pour étendre un système de fichiers monté nommé `/dev/xvda1`, utilisez la commande suivante.

```
[ec2-user ~]$ sudo resize2fs /dev/xvda1
```


Conseils pour le dépannage

- `resize2fs: Bad magic number in super-block while trying to open /dev/xvda1` : indique que le système de fichiers n'est pas Ext4. Pour vérifier le type de système de fichiers, utilisez la commande `df -hT`.
 - `open: No such file or directory while opening /dev/xvdb1` : indique que vous avez spécifié une partition incorrecte. Pour vérifier la partition, utilisez la commande `df -hT`.
 - `The filesystem is already 3932160 blocks long. Nothing to do!` : indique que le système de fichiers occupe déjà l'ensemble du volume. Si le volume ne comporte pas de partitions, [confirmez que la modification du volume a réussi](#). Si le volume comporte des partitions, assurez-vous que la partition a été étendue, comme décrit à l'étape 2.
- [Autre système de fichiers] Consultez la documentation de votre système de fichiers pour obtenir des instructions.
- c. Vérifiez que le système de fichiers a été étendu. Utilisez la commande `df -hT` et confirmez que la taille du système de fichiers est égale à la taille du volume.

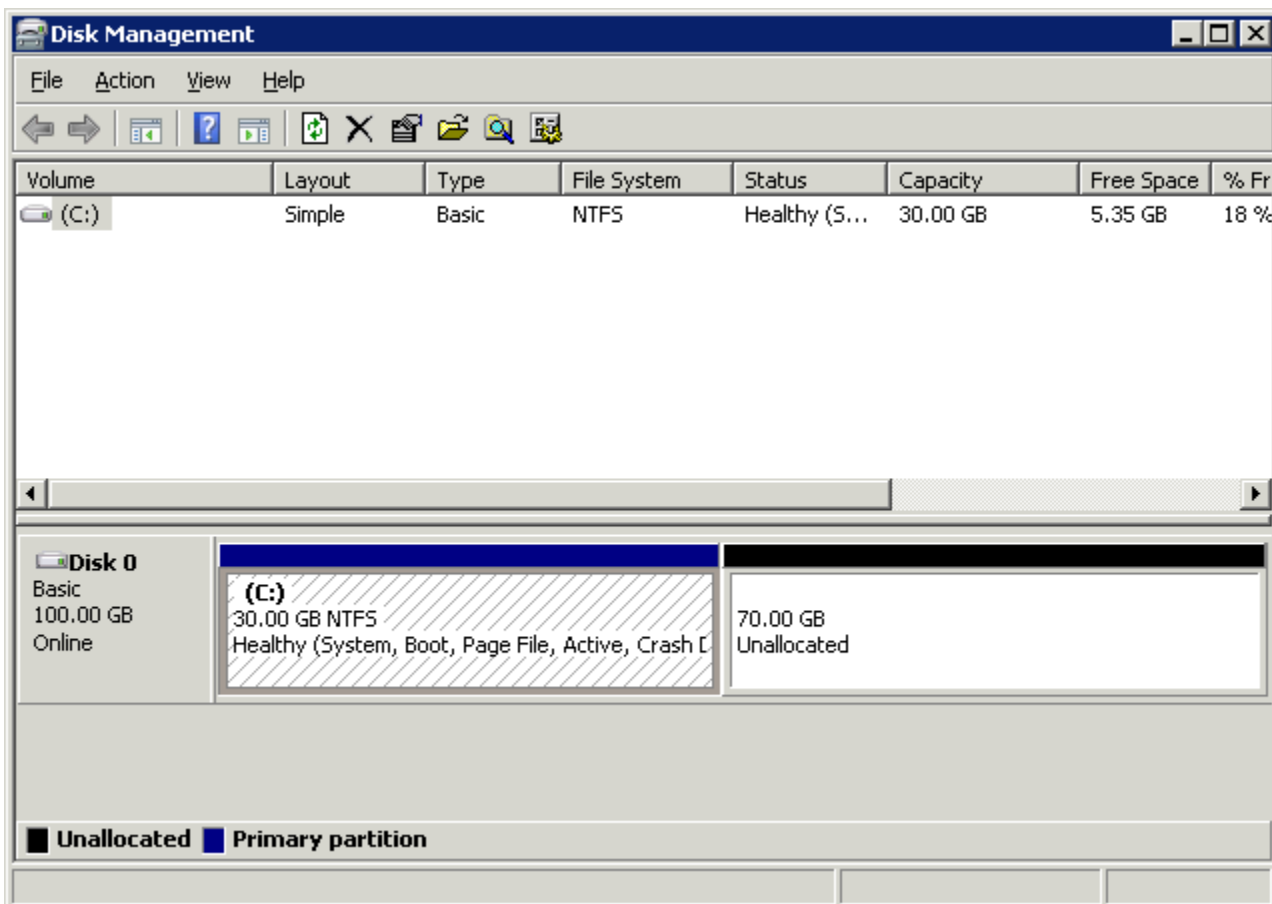
instances Windows

Utilisez l'une des méthodes suivantes pour étendre le système de fichiers sur une instance Windows.

Disk Management utility

Pour étendre un système de fichiers à l'aide de la gestion des disques

1. Avant d'étendre un système de fichiers qui contient des données critiques, une bonne pratique consiste à créer un instantané du volume qui le contient au cas où vous auriez besoin d'annuler vos modifications. Pour plus d'informations, consultez [Créer des instantanés Amazon EBS](#).
2. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance.
3. Dans la boîte de dialogue Exécuter, saisissez `diskmgmt.msc` et appuyez sur Entrée. L'utilitaire Gestion des disques s'ouvre.

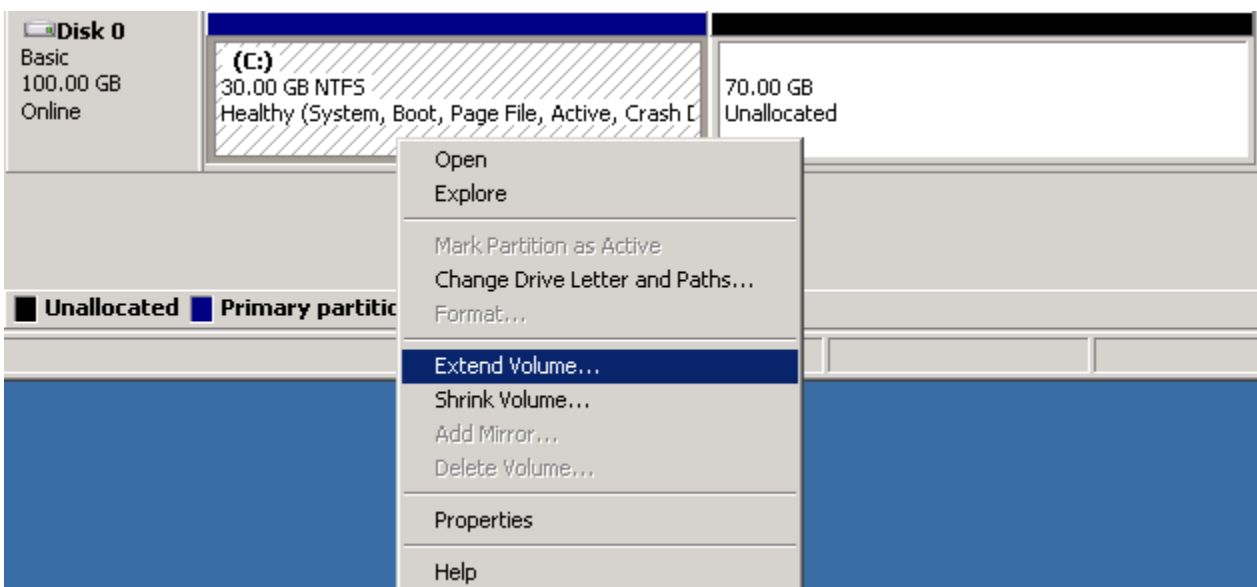


4. Dans le menu Gestion des disques, choisissez Action, Analyser les disques de nouveau.
5. Ouvrez le menu contextuel (clic droit) correspondant au disque étendu et choisissez Extension du volume.

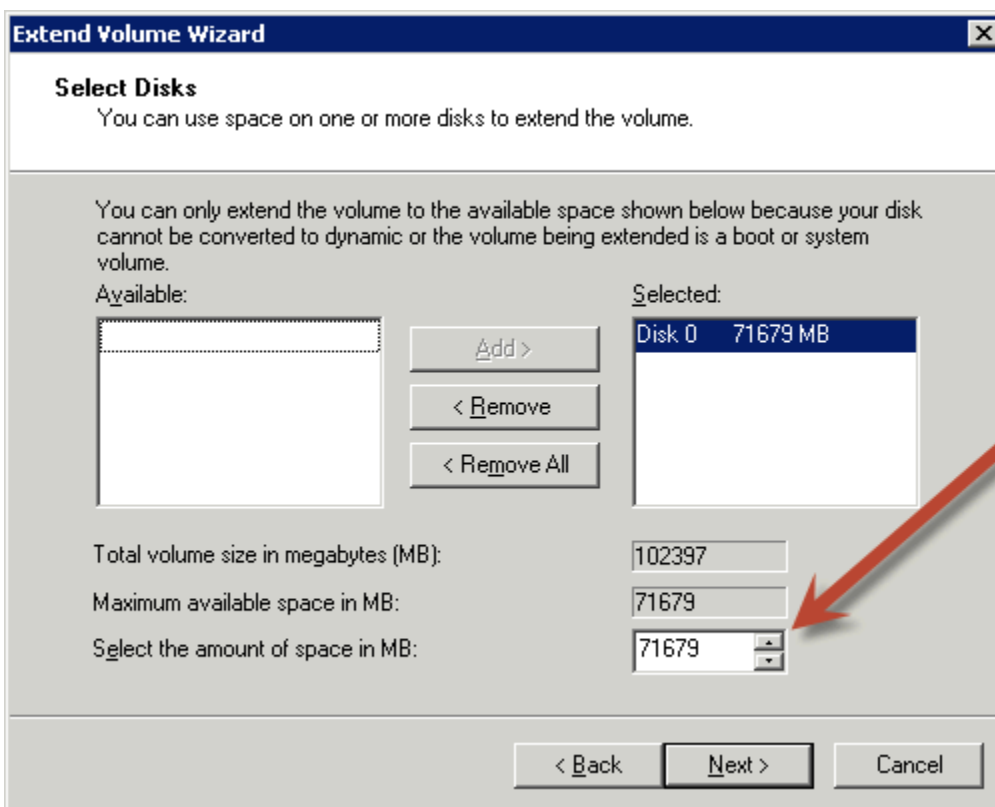
Note

Extension du volume peut être désactivé (grisé) si :

- L'espace non alloué n'est pas adjacent au lecteur. L'espace non alloué doit être adjacent au côté droit du disque que vous souhaitez étendre.
- Le volume utilise le style de partition MBR (Master Boot Record) et il a déjà une taille de 2 To. Les volumes qui utilisent MBR ne peuvent pas dépasser 2 To.



6. Dans l'Assistant Extension du volume, choisissez Suivant. Pour Select the amount of space in MB (Sélectionner la quantité d'espace en Mo), indiquez le nombre de méga-octets jusqu'auquel vous voulez étendre le volume. En règle générale, vous spécifiez l'espace disponible maximal. Le texte en surbrillance qui figure sous Sélectionné correspond à la quantité d'espace ajoutée, pas à la taille finale du volume. Exécutez l'assistant.



7. Si vous augmentez la taille d'un volume NVMe sur une instance qui ne possède pas le pilote NVMe AWS , vous devez redémarrer l'instance pour permettre à Windows de voir la nouvelle taille du volume. Pour plus d'informations sur l'installation du pilote AWS NVMe, consultez la section Pilotes [AWS NVMe](#).

PowerShell

Suivez la procédure suivante pour étendre un système de fichiers Windows à l'aide de PowerShell.

Pour étendre un système de fichiers à l'aide de PowerShell

1. Avant d'étendre un système de fichiers qui contient des données critiques, une bonne pratique consiste à créer un instantané du volume qui le contient au cas où vous auriez besoin d'annuler vos modifications. Pour plus d'informations, consultez [Créer des instantanés Amazon EBS](#).
2. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance.
3. Exécutez PowerShell en tant qu'administrateur.
4. Exécutez la `Get-Partition` commande. PowerShell renvoie le numéro de partition correspondant pour chaque partition, la lettre du lecteur, le décalage, la taille et le type. Notez la lettre de lecteur de la partition à étendre.
5. Exécutez la commande suivante pour effectuer une nouvelle analyse du disque.

```
"rescan" | diskpart
```

6. Exécutez la commande suivante en utilisant la lettre de lecteur que vous avez notée à l'étape 4 à la place de **<drive-letter>**. PowerShell renvoie la taille minimale et maximale de la partition autorisée, en octets.

```
Get-PartitionSupportedSize -DriveLetter <drive-letter>
```

7. Pour étendre la partition à une quantité spécifiée, exécutez la commande suivante, en entrant la nouvelle taille du volume à la place de **<size>**. Vous pouvez entrer la taille en KB, MB et GB, par exemple 50GB.

```
Resize-Partition -DriveLetter <drive-letter> -Size <size>
```

Pour étendre la partition à la taille maximale disponible, exécutez la commande suivante.

```
Resize-Partition -DriveLetter <drive-letter> -Size $(Get-PartitionSupportedSize
-DriveLetter <drive-letter>).SizeMax
```

Les PowerShell commandes suivantes présentent le flux complet de commandes et de réponses permettant d'étendre un système de fichiers à une taille spécifique.

```
PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset              Size  Type
-----
1                C            1048576             30 GB  IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset              Size  Type
-----
1                D            1048576             8 MB  IFS

PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin      SizeMax
-----
8388608 107372085248

PS C:\> Resize-Partition -DriveLetter D -Size 50GB
PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset              Size  Type
-----
1                C            1048576             30 GB  IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter  Offset              Size  Type
-----
1                D            1048576             50 GB  IFS
```

Les PowerShell commandes suivantes présentent le flux complet de commandes et de réponses permettant d'étendre un système de fichiers à la taille maximale disponible.

```

PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                Size Type
-----
1                C      1048576                30 GB IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                Size Type
-----
1                D      1048576                50 GB IFS

PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin      SizeMax
-----
59047936 107372085248

PS C:\> Resize-Partition -DriveLetter D -Size $(Get-PartitionSupportedSize -DriveLetter D).SizeMax
PS C:\> Get-Partition

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                Size Type
-----
1                C      1048576                30 GB IFS

DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                Size Type
-----
1                D      1048576               100 GB IFS

```

Détacher un volume Amazon EBS d'une instance Amazon EC2

Vous devez détacher un volume Amazon Elastic Block Store (Amazon EBS) d'une instance avant de pouvoir l'attacher à une autre instance ou le supprimer. Le détachement d'un volume n'affecte pas les données du volume.

Rubriques

- [Considérations](#)
- [Démonter et détacher un volume](#)

- [Dépannage](#)

Considérations

- Vous pouvez détacher un volume Amazon EBS d'une instance explicitement ou en mettant fin à l'instance. Toutefois, si l'instance est en cours d'exécution, vous devez d'abord démonter le volume à partir de l'instance.
- Si un volume EBS est le volume racine d'une instance, vous devez arrêter l'instance avant de pouvoir détacher le volume.
- Vous pouvez rattacher un volume que vous avez détaché (sans l'avoir démonté), mais celui-ci n'aura peut-être pas le même point de montage. S'il y avait des écritures en cours sur le volume au moment où il a été détaché, les données sur le volume peuvent ne pas être synchronisées.
- Une fois que vous avez détaché un volume, le stockage en volume vous est toujours facturé tant que la quantité de stockage dépasse la limite du niveau AWS gratuit. Vous devez supprimer un volume pour éviter de générer des frais supplémentaires. Pour plus d'informations, consultez [Supprimer un volume Amazon EBS](#).

Démonter et détacher un volume

Utilisez les procédures suivantes pour démonter et détacher un volume d'une instance. Cela peut être utile lorsque vous devez attacher le volume à une autre instance ou lorsque vous devez le supprimer.

Étapes

- [Étape 1 : Démonter le volume](#)
- [Étape 2 : Détacher le volume de l'instance](#)
- [Étape 3 : \(Instances Windows uniquement\) Désinstallez les emplacements des appareils hors ligne](#)

Étape 1 : Démonter le volume

Instances Linux

À partir de votre instance Linux, utilisez la commande suivante pour démonter l'unité `/dev/sdh`.

```
[ec2-user ~]$ sudo umount -d /dev/sdh
```

instances Windows

Depuis votre instance Windows, démontez le volume comme suit.

1. Démarrez l'utilitaire Gestion des disques.
 - (Windows Server 2012 et versions ultérieures) Dans la barre des tâches, choisissez (cliquez avec le bouton droit) sur le logo Windows et choisissez Gestion des disques.
 - (Windows Server 2008) Sélectionnez Start (Démarrer), Administrative Tools (Outils d'administration), Computer Management (Gestion des ordinateurs) et Disk Management (Gestion des disques).
2. Choisissez le disque (par exemple, choisissez (clic droit) Disque 1), puis choisissez Hors ligne. Attendez que l'état du disque passe à Hors connexion avant d'ouvrir la console Amazon EC2.

Étape 2 : Détacher le volume de l'instance

Pour détacher le volume de l'instance, utilisez l'une des méthodes suivantes :

Console

Pour détacher un volume EBS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume.
4. Choisissez Actions, puis Détachez le volume.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Detach.

AWS CLI

Pour détacher un volume EBS d'une instance

Après avoir démonté le volume, utilisez la commande [detach-volume](#).

```
aws ec2 detach-volume --volume-id vol-01234567890abcdef
```

PowerShell

Pour détacher un volume EBS d'une instance

Après avoir démonté le volume, utilisez l'[Dismount-EC2Volume](#) applet de commande.

```
Dismount-EC2Volume -VolumeId vol-01234567890abcdef
```

Étape 3 : (Instances Windows uniquement) Désinstallez les emplacements des appareils hors ligne

Lorsque vous démontez et détachez un volume d'une instance, Windows signale l'emplacement du périphérique comme étant hors connexion. L'emplacement du périphérique reste hors ligne après le rebooting, l'arrêt et le redémarrage de l'instance. Lorsque vous redémarrez l'instance, Windows peut monter l'un des volumes restants à l'emplacement du périphérique hors connexion. Le volume devient indisponible dans Windows. Pour éviter cela et pour vous assurer que tous les volumes sont connectés aux emplacements des appareils en ligne au prochain démarrage de Windows, effectuez les opérations suivantes :

1. Sur l'instance, ouvrez le Gestionnaire de périphériques.
2. Dans le Gestionnaire de périphériques, sélectionnez View (Affichage), Show hidden devices (Afficher les périphériques masqués).
3. Dans la liste des périphériques, développez le nœud Storage controllers (Contrôleurs de stockage).

Les emplacements de périphériques sur lesquels les volumes détachés ont été montés sont nommés AWS NVMe Elastic Block Storage Adapter et ils doivent être grisés.

4. Choisissez (cliquez avec le bouton droit de la souris) chaque emplacement d'appareil grisé nommé AWS NVMe Elastic Block Storage Adapter, sélectionnez Désinstaller l'appareil et choisissez Désinstaller.

Important

Ne cochez pas la case Delete the driver software for this device (Supprimer le pilote logiciel pour ce périphérique).

Dépannage

Voici des problèmes courants rencontrés lors du détachement de volumes, ainsi que la façon de les résoudre.

 Note

Pour vous prémunir contre la possibilité de perte de données, prenez un instantané de votre volume avant d'essayer de le démonter. Le détachement forcé d'un volume bloqué peut endommager le système de fichiers ou les données qu'il contient ou entraîner une incapacité d'attacher un volume à l'aide du même nom de périphérique, sauf si vous redémarrez l'instance.

- Si vous rencontrez des problèmes lors du détachement d'un volume à l'aide de la console Amazon EC2, il peut être utile d'utiliser la commande `describe-volumes` de l'interface de ligne de commande pour diagnostiquer le problème. Pour plus d'informations, consultez [describe-volumes](#).
- Si votre volume reste à l'état `detaching`, vous pouvez forcer le détachement en cliquant sur **Force Detach** (Forcer le détachement). Utilisez cette option uniquement comme dernier recours pour détacher un volume d'une instance en échec, ou si vous détachez un volume avec l'intention de le supprimer. L'instance n'a pas la possibilité de vider les caches du système de fichiers ou les métadonnées du système de fichiers. Si vous utilisez cette option, vous devez effectuer un contrôle du système de fichiers et des procédures de réparation.
- Si vous avez essayé de forcer le volume à se détacher plusieurs fois sur plusieurs minutes et qu'il reste à l'état `detaching`, vous pouvez envoyer une demande d'aide à [AWS re:Post](#). Pour aider à accélérer la résolution d'un problème, incluez l'ID du volume et décrivez les étapes que vous avez déjà effectuées.
- Lorsque vous essayez de détacher un volume qui est toujours monté, le volume peut se bloquer dans l'état `busy` lorsque vous tentez de le détacher. La sortie suivante de la commande `describe-volumes` présente un exemple de cette condition :

```
"Volumes": [  
  {  
    "AvailabilityZone": "us-west-2b",  
    "Attachments": [  
      {  
        "AttachTime": "2022-07-21T23:44:52.000Z",  
        "InstanceId": "i-1234567890abcdef0",  
        "VolumeId": "vol-01234567890abcdef",  
        "State": "busy",  
        "DeleteOnTermination": false,  
        "Device": "/dev/sdf"  
      }  
    ]  
  }  
]
```

```
    ...  
  }  
]
```

Lorsque vous rencontrez cet état, le détachement peut être retardé indéfiniment jusqu'à ce que vous démontiez le volume, forciez le détachement, redémarriez l'instance ou les trois.

Supprimer un volume Amazon EBS

Vous pouvez supprimer un volume Amazon EBS dont vous n'avez plus besoin. Une fois le volume supprimé, ses données sont perdues et il ne peut être attaché à aucune instance. Ainsi, avant la suppression, vous pouvez stocker un instantané du volume, que vous pourrez utiliser pour recréer le volume ultérieurement.

Vous ne pouvez pas supprimer un volume si celui-ci est attaché à une instance. Pour supprimer un volume, vous devez d'abord le détacher. Pour plus d'informations, consultez [Détacher un volume Amazon EBS d'une instance Amazon EC2](#).

Si vous supprimez un volume qui correspond à une règle de conservation de la corbeille, le volume est conservé dans la corbeille au lieu d'être immédiatement supprimé. Pour plus d'informations, voir [Corbeille](#).

Console

Pour supprimer un volume EBS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume. Vérifiez que le volume est à l'état Disponible.
4. Choisissez Actions, puis Supprimer le volume.

Si cette option est désactivée, le volume est attaché à une instance et ne peut pas être supprimé.

5. Lorsque vous êtes invité à confirmer, saisissez **delete**, puis choisissez Delete (Supprimer).

AWS CLI

Pour vérifier si un volume EBS est en cours d'utilisation

Utilisez la commande [describe-volumes](#). Si le volume est en cours d'utilisation, son état est `in-use`. Sinon, la valeur est `available`.

```
aws ec2 describe-volumes \
  --volume-id vol-01234567890abcdef \
  --query Volumes[*].State \
  --output text
```

Pour supprimer un volume EBS

Utilisez la commande [delete-volume](#).

```
aws ec2 delete-volume --volume-id vol-01234567890abcdef
```

PowerShell

Pour vérifier si un volume EBS est en cours d'utilisation

Utilisez l'applet de commande [Get-EC2Volume](#). Si le volume est en cours d'utilisation, son état est `in-use`. Sinon, la valeur est `available`.

```
(Get-EC2Volume `
  -VolumeId vol-01234567890abcdef).State.Value
```

Pour supprimer un volume EBS

Utilisez l'applet de commande [Remove-EC2Volume](#).

```
Remove-EC2Volume -VolumeId vol-01234567890abcdef
```

Remplacer un volume Amazon EBS à l'aide d'un instantané

Les instantanés Amazon EBS constituent l'outil de sauvegarde idéal sur Amazon EC2 en raison de leur vitesse, de leur commodité et de leur coût. Lorsque vous créez un volume à partir d'un instantané, vous recréez son état à un moment précis dans le temps avec les données sauvegardées intactes jusqu'à ce moment là. En attachant un volume créé à partir d'un instantané à une instance, vous pouvez dupliquer des données dans plusieurs régions, créer des environnements de test, remplacer un volume de production endommagé ou corrompu dans son intégralité ou récupérer

des fichiers et des répertoires spécifiques et les transférer vers un autre volume attaché. Pour plus d'informations, consultez [Instantanés Amazon EBS](#).

Vous pouvez suivre les procédures ci-après pour remplacer un volume Amazon EBS par un autre volume créé à partir d'un instantané antérieur du volume.

Exigence

Vous devez créer le volume dans la même zone de disponibilité que votre instance. Les volumes doivent être attachés à des instances situées dans la même zone de disponibilité.

Console

Pour remplacer un volume

1. Créez un volume à partir de l'instantané et notez l'ID du nouveau volume. Pour plus d'informations, consultez [Créez un volume Amazon EBS](#).
2. Sur la page Instances, sélectionnez l'instance sur laquelle vous souhaitez remplacer le volume et notez l'ID de l'instance.

Alors que l'instance est toujours sélectionnée, choisissez l'onglet Storage (Stockage). Dans la section Block devices (Périphériques de bloc), recherchez le volume à remplacer et notez le nom du périphérique pour le volume, par exemple /dev/sda1.

3. Dans l'onglet Stockage, choisissez l'ID du volume, puis [démontez et détachez le volume de l'instance](#).
4. Sélectionnez le nouveau volume que vous avez créé à l'étape 1 et choisissez Actions, Attach volume (Attacher un volume).

Pour Instance et Device name (Nom de périphérique), saisissez l'ID d'instance et le nom de périphérique que vous avez noté à l'étape 2, puis choisissez Attach volume (Attacher le volume).

5. Connectez-vous à votre instance et montez le volume. Pour plus d'informations, consultez [Mettre un volume Amazon EBS à disposition pour utilisation](#).

AWS CLI

Pour remplacer un volume

1. Créez un volume à partir de l'instantané. Utilisez la [commande](#) `create-volume` avec l'option `--snapshot-id`. Pour `--availability-zone`, spécifiez la même zone de disponibilité que l'instance. Notez l'ID du nouveau volume dans la sortie.

```
aws ec2 create-volume \  
  --volume-type gp3 \  
  --snapshot-id snap-0abcdef1234567890 \  
  --availability-zone us-east-1a
```

2. Obtenez le nom du périphérique du volume à remplacer. Utilisez la commande [describe-instances](#). Pour `--instance-ids`, spécifiez l'ID de l'instance dont le volume doit être remplacé. Notez le nom de l'appareil et l'ID du volume à remplacer.

```
aws ec2 describe-instances \  
  --instance-ids i-1234567890abcdef0 \  
  --query Reservations[].Instances[].BlockDeviceMappings
```

3. Détachez le volume à remplacer de l'instance. Utilisez la commande [detach-volume](#).

```
aws ec2 detach-volume --volume-id vol-xxxxxxxxxxxxxxxxxx
```

4. Attachez le volume de remplacement à l'instance. Utilisez la commande [attach-volume](#). Pour `--volume-id`, spécifiez l'ID du volume de remplacement. Pour `--instance-id`, spécifiez l'ID de l'instance à laquelle vous souhaitez attacher le volume. Pour `--device`, spécifiez le même nom de périphérique que celui que vous avez noté précédemment.

```
aws ec2 attach-volume \  
  --volume-id vol-01234567890abcdef \  
  --instance-id i-1234567890abcdef0 \  
  --device /dev/sdf
```

5. Connectez-vous à votre instance et montez le volume. Pour plus d'informations, consultez [Mettre un volume Amazon EBS à disposition pour utilisation](#).

PowerShell

Pour remplacer un volume

1. Créez un volume à partir de l'instantané. Utilisez l'[New-EC2Volume](#) applet de commande avec l'-SnapshotIdoption. Pour -AvailabilityZone, spécifiez la même zone de disponibilité que l'instance. Notez l'ID du nouveau volume dans la sortie.

```
New-EC2Volume `
  -VolumeType gp3 `
  -SnapshotId snap-0abcdef1234567890 `
  -AvailabilityZone us-east-1a
```

2. Obtenez le nom du périphérique du volume à remplacer. Utilisez l'applet de commande [Get-EC2Instance](#). Pour -InstanceId, spécifiez l'ID de l'instance dont le volume doit être remplacé. Notez le nom de l'appareil et l'ID du volume à remplacer.

```
(Get-EC2Instance `
  -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings | `
  Format-Table DeviceName, @{Name="VolumeId";Expression={$_.Ebs.VolumeId}}
```

3. Détachez le volume à remplacer de l'instance. Utilisez l'applet de commande [Dismount-EC2Volume](#).

```
DismountEC2Volume -VolumeId vol-xxxxxxxxxxxxxxxxxxx
```

4. Attachez le volume de remplacement à l'instance. Utilisez l'applet de commande [Add-EC2Volume](#). Pour -VolumeId, spécifiez l'ID du volume de remplacement. Pour -InstanceId, spécifiez l'ID de l'instance à laquelle vous souhaitez attacher le volume. Pour -Device, spécifiez le même nom de périphérique que celui que vous avez noté précédemment.

```
Add-EC2Volume `
  -VolumeId vol-01234567890abcdef `
  -InstanceId i-1234567890abcdef0 `
  -Device /dev/sdf
```

5. Connectez-vous à votre instance et montez le volume. Pour plus d'informations, consultez [Mettre un volume Amazon EBS à disposition pour utilisation](#).

Vérifications de l'état des volumes Amazon EBS

Les contrôles de statut de volume vous permettent de mieux comprendre, suivre et gérer les incohérences potentielles des données d'un volume Amazon EBS. Ils sont destinés à vous fournir les informations dont vous avez besoin pour déterminer si vos volumes Amazon EBS rencontrent des problèmes et pour vous aider à contrôler comment un volume potentiellement incohérent est géré.

Les contrôles de statut de volume sont exécutés automatiquement toutes les cinq minutes et renvoie un statut de réussite ou d'échec. Si tous les contrôles réussissent, le statut du volume est `ok`. Si un contrôle échoue, le statut du volume est `impaired`. Si le statut est `insufficient-data`, il se peut que les contrôles soient toujours en cours sur le volume. Vous pouvez afficher les résultats des contrôles de statut de volume pour identifier les volumes confrontés à des problèmes et prendre les actions nécessaires.

Lorsqu'Amazon EBS détermine que les données d'un volume sont potentiellement incohérentes, il désactive par défaut toutes les instances EC2 connectées I/O au volume, ce qui permet d'éviter toute corruption des données. Après avoir été I/O désactivé, la prochaine vérification de l'état du volume échoue et l'état du volume est `impaired`. En outre, un événement vous indiquera qu'il I/O est désactivé et que vous pouvez résoudre le problème d'altération du volume en I/O l'activant. EBS attend que vous l'activiez I/O pour vous permettre de décider si vous souhaitez continuer à autoriser vos instances à utiliser le volume ou si vous souhaitez exécuter un contrôle de cohérence à l'aide d'une commande, telle que `fsck` (instances Linux) ou `chkdsk` (instances Windows), avant de procéder.

Note

Le statut du volume s'appuie sur les vérifications de statut du volume et ne reflète pas l'état du volume. Par conséquent, l'état du volume n'indique pas les volumes dans `error` l'état (par exemple, lorsqu'un volume ne peut pas être accepté) I/O. Pour obtenir des informations sur l'état du volume, veuillez consulter [États du volume](#).

Si la cohérence d'un volume particulier n'est pas un problème et que vous préférez que le volume soit immédiatement disponible s'il est altéré, vous pouvez modifier le comportement par défaut en configurant le volume pour qu'il soit activé I/O automatiquement. Si vous activez l'attribut de volume d'Auto-Enable E/S (`autoEnableIO` dans l'API), la vérification de l'état du volume continue de réussir. En outre, vous verrez un événement vous indiquant que le volume a été jugé potentiellement

incohérent, mais qu'il a I/O été automatiquement activé. Cela vous permet de vérifier la cohérence du volume ou de le remplacer ultérieurement.

La vérification de l'état des I/O performances compare les performances réelles du volume aux performances attendues d'un volume. Il vous prévient si le volume se comporte en-deçà des attentes. Cette vérification d'état n'est disponible que pour les volumes SSD IOPS provisionnés (io1 et io2) et les volumes SSD polyvalent (gp3) attachés à une instance. La vérification d'état n'est pas valide pour les volumes SSD polyvalent (gp2), HDD à débit optimisé (st1), HDD à froid (sc1), ou magnétique (standard). Le contrôle de l'état des I/O performances est effectué une fois par minute et CloudWatch collecte ces données toutes les 5 minutes. Cela peut prendre jusqu'à 5 minutes à partir du moment où vous associez un io2 volume io1 ou à une instance pour que la vérification de l'état rende compte de l'état I/O des performances.

 Important

Lors de l'initialisation de volumes SSD IOPS provisionnés qui ont été restaurés à partir de snapshots, les performances du volume peuvent chuter en dessous de 50 % de leur niveau attendu, ce qui entraîne l'affichage d'un warning état lors de la vérification de l'état des performances. I/O Cette situation est attendue et vous pouvez ignorer l'état warning des volumes Provisioned IOPS SSD lorsque vous les initialisez. Pour plus d'informations, consultez [Initialiser manuellement les volumes après leur création](#).

Le tableau suivant répertorie les statuts des volumes Amazon EBS.

Statut du volume	I/O état activé	I/O état des performances (io1io2, et gp3 volumes uniquement)
ok	Activé (I/O Activé ou I/O Auto-Enabled)	Normal (performances du volume telles qu'attendues)
warning	Activé (I/O Activé ou I/O Auto-Enabled)	Dégradé (performances du volume inférieures aux attentes)

Statut du volume	I/O état activé	I/O état des performances (io1 io2 , et gp3 volumes uniquement)
		Profondément dégradé (performances du volume bien inférieures aux attentes)
impaired	Activé (I/O Activé ou I/O Auto-Enabled) Désactivé (le volume est hors ligne et en attente de restauration, ou attend que vous l'activiez I/O)	Interrompu (performances du volume profondément impactées) Non disponible (Impossible de déterminer les I/O performances car il I/O est désactivé)
insufficient-data	Activé (I/O Activé ou I/O Auto-Enabled) Données insuffisantes	Données insuffisantes

Console

Pour afficher les contrôles de statut

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.

La colonne Volume Status (Statut du volume) affiche le statut opérationnel de chaque volume.

3. Pour afficher les détails du statut d'un volume spécifique, sélectionnez-le dans la grille et choisissez l'onglet Status checks (Vérifications de l'état).
4. Si vous avez un volume dont la vérification de l'état a échoué (l'état est impaired), consultez [Travaillez avec un volume Amazon EBS altéré](#).

Vous pouvez aussi choisir Événements dans le navigateur pour afficher tous les événements de vos instances et volumes. Pour plus d'informations, consultez [Événements liés au volume Amazon EBS](#).

AWS CLI

Pour afficher les informations de statut du volume

Utilisez la commande [describe-volume-status](#).

```
aws ec2 describe-volume-status --volume-ids vol-01234567890abcdef
```

Utilisez l'exemple suivant pour identifier les volumes altérés.

```
aws ec2 describe-volume-status --filters Name=volume-status.status,Values=impaired
```

PowerShell

Pour afficher les informations de statut du volume

Utilisez l'applet de commande [Get-EC2VolumeStatus](#).

```
Get-EC2VolumeStatus -VolumeId vol-01234567890abcdef
```

Utilisez l'exemple suivant pour identifier les volumes altérés.

```
Get-EC2VolumeStatus -Filter @{Name="volume-status.status"; Values="impaired"}
```

Événements liés au volume Amazon EBS

Lorsqu'Amazon EBS détermine que les données d'un volume sont potentiellement incohérentes, il désactive le volume I/O à partir de toutes les instances EC2 connectées par défaut. Il s'ensuit que le contrôle du statut du volume échoue et qu'un événement de statut de volume est créé indiquant la raison de l'échec.

Pour I/O activer automatiquement un volume présentant des incohérences de données potentielles, modifiez le paramètre de l'attribut de volume Auto-Enabled IO (`autoEnableIO` dans l'API). Pour plus d'informations sur la modification de cet attribut, consultez [Travaillez avec un volume Amazon EBS altéré](#).

Chaque événement comprend une heure de début qui indique l'heure à laquelle l'événement s'est produit et une durée qui indique la durée pendant I/O laquelle le volume a été désactivé. L'heure de fin est ajoutée à l'événement lorsque I/O le volume est activé.

Événements relatifs à l'état du volume

Awaiting Action: Enable IO

Les données de volume sont potentiellement incohérentes. I/O est désactivé pour le volume jusqu'à ce que vous l'activiez explicitement. La description de l'événement est modifiée une IO Enabled fois que vous l'avez explicitement activé I/O.

IO Enabled

I/O les opérations ont été explicitement activées pour ce volume.

IO Auto-Enabled

I/O les opérations étaient automatiquement activées sur ce volume après la survenance d'un événement. Nous vous recommandons de vérifier leurs incohérences avant de continuer à utiliser les données.

Normal

Pour les volumes io1, io2 et gp3 uniquement. Performances du volume telles qu'attendues.

Degraded

Pour les volumes io1, io2 et gp3 uniquement. Performances du volume inférieures aux attentes.

Severely Degraded

Pour les volumes io1, io2 et gp3 uniquement. Performances du volume bien inférieures aux attentes.

Stalled

Pour les volumes io1, io2 et gp3 uniquement. Performances du volume profondément impactées.

Si vous avez un volume qui I/O est désactivé, consultez [Travaillez avec un volume Amazon EBS altéré](#). Si les I/O performances de votre volume sont inférieures à la normale, il peut s'agir d'une condition temporaire due à une action que vous avez entreprise (par exemple, créer un instantané

d'un volume pendant les pics d'utilisation, exécuter le volume sur une instance ne prenant pas en charge la I/O bande passante requise, accéder aux données du volume pour la première fois, etc.).

Console

Pour afficher les événements de vos volumes

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Événements. Tous les volumes et instances ayant des événements sont affichés.
3. Vous pouvez filtrer par volume pour n'afficher que le statut de volume. Vous pouvez aussi filtrer sur des types de statut spécifiques.
4. Sélectionnez un volume pour afficher son événement spécifique.

AWS CLI

Pour afficher les événements de vos volumes

Utilisez la commande [describe-volume-status](#).

```
aws ec2 describe-volume-status --volume-ids vol-01234567890abcdef
```

PowerShell

Pour afficher les événements de vos volumes

Utilisez l'applet de commande [Get-EC2VolumeStatus](#).

```
Get-EC2VolumeStatus -VolumeId vol-01234567890abcdef
```

Travaillez avec un volume Amazon EBS altéré

Cette section présente vos options si un volume est dégradé flotee que ses données sont potentiellement incohérentes.

Options

- [Option 1 : exécuter un contrôle de cohérence sur le volume attaché à son instance](#)

- [Option 2 : exécuter un contrôle de cohérence sur le volume à l'aide d'une autre instance](#)
- [Option 3 : supprimer le volume si vous n'en avez plus besoin](#)

Option 1 : exécuter un contrôle de cohérence sur le volume attaché à son instance

L'option la plus simple consiste à activer I/O puis à effectuer un contrôle de cohérence des données sur le volume alors que celui-ci est toujours attaché à son instance Amazon EC2.

Pour exécuter un contrôle de cohérence sur un volume attaché

1. Arrêtez l'utilisation du volume par les applications.
2. Activez I/O sur le volume. Utilisez l'une des méthodes suivantes.

Console

I/O Pour activer un volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Events.
3. Sélectionnez le volume.
4. Choisissez Actions, Activer I/O.

AWS CLI

I/O Pour activer un volume

Utilisez la commande [enable-volume-io](#).

```
aws ec2 enable-volume-io --volume-id vol-01234567890abcdef
```

PowerShell

I/O Pour activer un volume

Utilisez l'applet de commande [Enable-EC2VolumeIO](#).

```
Enable-EC2VolumeIO -VolumeId vol-01234567890abcdef
```

3. Vérifiez les données du volume.

- a. Exécutez la commande `fsck` (instances Linux) ou `chkdsk` (instances Windows).
- b. (Facultatif) Recherchez dans les journaux des applications journaux système disponibles les messages d'erreur appropriés.
- c. Si le volume est réduit pendant plus de 20 minutes, vous pouvez contacter le centre d' AWS assistance. Sélectionnez Dépannage puis, dans la boîte de dialogue Dépanner les contrôles de statut, sélectionnez Contactez Support pour soumettre une demande de support.

Option 2 : exécuter un contrôle de cohérence sur le volume à l'aide d'une autre instance

Utilisez la procédure suivante pour vérifier le volume en dehors de votre environnement de production.

Important

Cette procédure peut entraîner la perte de l'écriture I/Os suspendue lorsque le volume I/O a été désactivé.

Pour exécuter un contrôle de cohérence sur un volume isolé

1. Arrêtez l'utilisation du volume par les applications.
2. Détachez le volume de l'instance. Pour plus d'informations, consultez [Détacher un volume Amazon EBS d'une instance Amazon EC2](#).
3. Activez I/O sur le volume. Utilisez l'une des méthodes suivantes.

Console

I/O Pour activer un volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Events.
3. Sélectionnez le volume que vous avez détaché à l'étape précédente.
4. Choisissez Actions, Activer I/O.

AWS CLI

I/O Pour activer un volume

Utilisez la commande [enable-volume-io](#).

```
aws ec2 enable-volume-io --volume-id vol-01234567890abcdef
```

PowerShell

I/O Pour activer un volume

Utilisez l'applet de commande [Enable-EC2VolumeIO](#).

```
Enable-EC2VolumeIO -VolumeId vol-01234567890abcdef
```

4. Attachez le volume à une autre instance. Pour plus d'informations, consultez [Lancer votre instance](#) et [Attacher un volume Amazon EBS à une instance Amazon EC2](#).
5. Vérifiez les données du volume.
 - a. Exécutez la commande fsck (instances Linux) ou chkdsk (instances Windows).
 - b. (Facultatif) Recherchez dans les journaux des applications journaux système disponibles les messages d'erreur appropriés.
 - c. Si le volume est réduit pendant plus de 20 minutes, vous pouvez contacter le centre d'AWS assistance. Sélectionnez Dépannage puis, dans la boîte de dialogue de dépannage, sélectionnez Contactez Support pour soumettre une demande de support.

Option 3 : supprimer le volume si vous n'en avez plus besoin

Si vous voulez supprimer le volume de votre environnement, supprimez-le simplement. Pour plus d'informations sur la suppression d'un volume, consultez [Supprimer un volume Amazon EBS](#).

Si vous avez un instantané récent qui sauvegarde les données sur le volume, vous pouvez créer un volume à partir de l'instantané. Pour plus d'informations, consultez [Créez un volume Amazon EBS](#).

Auto-enable I/O pour les volumes Amazon EBS altérés

Lorsqu'Amazon EBS détermine que les données d'un volume sont potentiellement incohérentes, il désactive le volume I/O à partir de toutes les instances EC2 connectées par défaut. Il s'ensuit que le contrôle du statut du volume échoue et qu'un événement de statut de volume est créé indiquant la raison de l'échec. Si la cohérence d'un volume particulier n'est pas un problème et que vous préférez que le volume soit immédiatement disponible s'il est altéré, vous pouvez modifier le comportement par défaut en configurant le volume pour qu'il soit activé I/O automatiquement. Si vous activez l'attribut de volume d'Auto-Enabled E/S (`autoEnableIO` dans l'API), la I/O liaison entre le volume et l'instance est automatiquement réactivée et la vérification de l'état du volume sera réussie. En outre, un événement vous indiquera que le volume était dans un état potentiellement incohérent, mais qu'il a I/O été automatiquement activé. Quand cet événement se produit, vous devez vérifier la cohérence du volume et le remplacer si nécessaire. Pour plus d'informations, consultez [Événements liés au volume Amazon EBS](#).

Console

Pour afficher l'attribut Auto-Enabled IO d'un volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume et choisissez Status Checks (Vérifications de l'état).

Le Auto-enabled I/O champ affiche le réglage actuel (Activé ou Désactivé) pour le volume sélectionné.

Pour modifier l'attribut Auto-Enabled IO d'un volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume et choisissez Actions, Gestion activée automatiquement I/O.
4. I/O Pour activer automatiquement un volume réduit, cochez la case Auto-enable I/O pour les volumes altérés. Pour désactiver la fonction, décochez la case.
5. Choisissez Mettre à jour.

AWS CLI

Pour afficher l'attribut AutoEnable IO d'un volume

Utilisez la commande [describe-volume-attribute](#).

```
aws ec2 describe-volume-attribute \  
  --attribute autoEnableIO \  
  --volume-id vol-01234567890abcdef
```

Voici un exemple de sortie.

```
{  
  "AutoEnableIO": {  
    "Value": true  
  },  
  "VolumeId": "vol-01234567890abcdef"  
}
```

Pour modifier l'attribut autoEnableIO d'un volume

Utilisez la commande [modify-volume-attribute](#).

```
aws ec2 modify-volume-attribute \  
  --auto-enable-io \  
  --volume-id vol-01234567890abcdef
```

PowerShell

Pour afficher l'attribut AutoEnable IO d'un volume

Utilisez l'applet de commande [Get-EC2VolumeAttribute](#).

```
(Get-EC2VolumeAttribute `\  
  -Attribute autoEnableIO `\  
  -VolumeId vol-01234567890abcdef).AutoEnableIO
```

Voici un exemple de sortie.

```
True
```

Pour modifier l'attribut autoEnableIO d'un volume

Utilisez l'applet de commande [Edit-EC2VolumeAttribute](#).

```
Edit-EC2VolumeAttribute `
  -AutoEnableIO $true `
  -VolumeId vol-01234567890abcdef
```

Tests de défaillance sur Amazon EBS

AWS Fault Injection Service (AWS FIS) est un service entièrement géré qui vous aide à effectuer des expériences d'injection de défauts sur vos AWS charges de travail. Grâce aux actions EBS AWS FIS, vous pouvez tester la façon dont vos applications réagissent aux défaillances de stockage qui peuvent entraîner des I/O interruptions et une dégradation des performances de vos volumes. Cet environnement de test contrôlé vous permet d'observer comment vos applications réagissent aux interruptions afin d'identifier les faiblesses de votre architecture et d'améliorer la résilience globale de vos applications. À l'aide de l' I/O action de pause et de l'action d'injection de latence, vous pouvez tester vos mécanismes de surveillance et de restauration tels que les CloudWatch alarmes Amazon et les flux de travail de basculement, et améliorer la résilience de vos applications critiques face aux défaillances de stockage. Pour plus d'informations à ce sujet AWS FIS, consultez le Guide de [AWS Fault Injection Service l'utilisateur](#).

Expériences disponibles

Amazon EBS prend actuellement en charge deux injections de AWS FIS défauts :

- [Suspendre l'injection par I/O défaut](#)
- [Injection de latence](#)

Considérations

Les considérations suivantes s'appliquent :

- Tous les types de volumes Amazon EBS sont pris en charge. Les volumes racine et les volumes de données sont pris en charge. Les volumes de stockage d'instances ne sont pas pris en charge.
- Les volumes doivent être attachés aux instances [Nitro-based](#) EC2.
- Vos volumes reprendront leur I/O performance initiale une fois l'expérience terminée, en fonction de sa durée. Vous pouvez également arrêter une expérience en cours avant qu'elle ne soit

terminée. Vous pouvez également créer une condition d'arrêt pour arrêter l'expérience si elle atteint un seuil que vous définissez dans une CloudWatch alarme.

- Vous pouvez l'utiliser AWS FIS avec les volumes Multi-Attach activés. Toutes les instances associées sont touchées. Vous ne pouvez pas sélectionner une pièce jointe d'instance de volume spécifique pour les expériences.
- Le FIS n'est actuellement pas disponible dans les zones locales, les avant-postes ou les zones de longueur d'onde.
- Vous pouvez tester simultanément jusqu'à 5 volumes dans la même zone de disponibilité lorsque vous spécifiez des ARN de volume dans la console.
- Vous ne pouvez pas l'utiliser AWS FIS avec des volumes créés dans une Outpost, dans une AWS Wavelength zone ou dans une zone locale.

Suspendre l'injection par I/O défaut

Utilisez AWS Fault Injection Service et l' I/O action Pause pour vous arrêter temporairement I/O entre un volume Amazon EBS et les instances auxquelles il est attaché afin de tester la façon dont vos charges de travail gèrent I/O les interruptions.

Pour plus d'informations à ce sujet AWS FIS, consultez le Guide de [AWS Fault Injection Service l'utilisateur](#).

Considérations

Tenez compte des considérations suivantes pour suspendre le volume I/O :

- I/O La pause est prise en charge sur tous les types d'[Nitro-based instances](#).
- Pour tester la configuration du délai d'attente de votre système d'exploitation, définissez une durée d'expérience égale ou supérieure à la valeur spécifiée pour `nvme_core.io_timeout`. Pour plus d'informations, consultez [Délai de I/O fonctionnement NVMe pour les volumes Amazon EBS](#).
- Si vous conduisez I/O jusqu'à un volume en I/O pause, voici ce qui se produit :
 - Le statut du volume passe à `impaired` dans les 120 secondes. Pour plus d'informations, consultez [Vérifications de l'état des volumes Amazon EBS](#).
 - La CloudWatch métrique pour `VolumeStalledIOCheck` sera 1 si le volume I/O est suspendu pendant plus de 60 secondes. Pour plus d'informations, consultez [Métriques pour les volumes Amazon EBS](#).

- Les CloudWatch mesures relatives à la longueur de la file d'attente (VolumeQueueLength) seront différentes de zéro. Toutes les alarmes et tous les contrôles doivent surveiller une profondeur de file d'attente non nulle.
- Les CloudWatch mesures pour VolumeReadOps ou VolumeWriteOps seront 0, ce qui indique que le volume n'est plus en cours de traitement I/O.

Vous pouvez effectuer une expérience de base à partir de la console Amazon EC2, ou vous pouvez effectuer des expériences plus avancées à l'aide de la AWS FIS console. Pour plus d'informations sur la réalisation d'expériences avancées à l'aide de la AWS FIS console, consultez les [AWS FIS](#) didacticiels du Guide de AWS Fault Injection Service l'utilisateur.

Pour réaliser une expérience de base à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume pour lequel vous souhaitez faire une pause I/O et choisissez Actions, Injection par défaut, Suspendre le volume I/O.
4. Dans Durée, entrez la durée pendant laquelle vous souhaitez faire une pause I/O entre le volume et les instances. Le champ situé à côté de la liste déroulante Durée indique la durée au format ISO 8601.
5. Dans la section Accès au service, sélectionnez le rôle de service IAM AWS FIS à assumer pour réaliser l'expérience. Vous pouvez utiliser le rôle par défaut ou un rôle existant que vous avez créé. Pour plus d'informations, consultez [Création d'un rôle IAM pour les expériences AWS FIS](#).
6. Choisissez Suspendre le volume I/O. Lorsque vous y êtes invité, entrez start dans le champ de confirmation et choisissez Commencer l'expérience.
7. Surveillez la progression et l'impact de votre expérience. Pour plus d'informations, consultez [Surveillance de AWS FIS](#) dans le Guide de l'utilisateur AWS FIS .

Injection de latence

Utilisez l'action Latency Injection (aws:ebs:volume-io-latency) AWS FIS pour simuler I/O une latence élevée sur vos volumes Amazon EBS afin de tester la façon dont vos applications réagissent à la dégradation des performances de stockage. Cette action vous permet de spécifier la valeur de latence à injecter ainsi que le pourcentage de I/O cette valeur qui sera impacté sur le volume cible. Avec AWS FIS, vous pouvez utiliser des modèles d'expérience de latence préconfigurés pour

commencer à tester les différents modèles de I/O latence qui peuvent être observés lors de pannes de stockage. Ces modèles sont conçus comme un ensemble initial de scénarios que vous pouvez utiliser pour introduire des interruptions dans vos applications afin de tester la résilience. Ils ne sont pas conçus pour englober tous les types d'impact que vos applications peuvent subir dans le monde réel. Nous vous recommandons de les adapter pour exécuter plusieurs tests différents en fonction des besoins de performances de vos applications. Vous pouvez personnaliser les modèles disponibles ou créer de nouveaux modèles d'expérience pour tester les exigences spécifiques de votre application.

Pre-configured modèles d'expériences de latence

Amazon EBS fournit les modèles d'expérience de latence suivants via la console EBS et la bibliothèque de [AWS FIS scénarios](#). Vous pouvez utiliser ces modèles directement sur vos volumes cibles pour exécuter une expérience d'injection de latence.

- **Latence prolongée** : simule une latence constante. Cette expérience utilise une action d'injection de latence et a une durée totale de 15 minutes. Cette expérience simule une latence persistante sur 50 % de la lecture I/O et 100 % de l'écriture I/O : 500 ms pendant 15 minutes.
- **Latence croissante** : simule une augmentation progressive de la latence. Cette expérience utilise cinq actions d'injection de latence et a une durée totale de 15 minutes. Cette expérience simulera une augmentation progressive de la latence sur 10 % de la lecture I/O et 25 % de l'écriture I/O : 50 ms pendant 3 minutes, 200 ms pendant 3 minutes, 700 ms pendant 3 minutes, 1 seconde pendant 3 minutes et 15 secondes pendant 3 minutes.
- **Latence intermittente** : simule de brusques pics de latence intermittents entrecoupés de périodes de rétablissement. Cette expérience utilise trois actions d'injection de latence et a une durée totale de 15 minutes. Cette expérience simulera trois pics de latence sur 0,1 % de la lecture et de l'écriture I/O : un pic de 30 secondes qui dure 1 minute, un pic de 10 secondes qui dure 2 minutes et un pic de 20 secondes qui dure 2 minutes. Il y aura des périodes de récupération de 5 minutes entre chaque pic de latence.
- **Latence décroissante** : simule une diminution progressive de la latence. Cette expérience utilise cinq actions d'injection de latence et a une durée totale de 15 minutes. Cette expérience simulera une diminution progressive de la latence sur 10 % de la lecture I/O et de l'écriture I/O : 20 secondes pendant 3 minutes, 5 secondes pendant 3 minutes, 900 ms pendant 3 minutes, 300 ms pendant 3 minutes et 40 ms pendant 3 minutes.

Personnalisez les scénarios préconfigurés

Vous pouvez personnaliser les modèles préconfigurés ci-dessus ou créer vos propres nouveaux modèles d'expérience à l'aide des paramètres personnalisables suivants.

- `readIOPercentage`— Pourcentage d' I/O opérations de lecture pour lesquelles une latence sera injectée. Il s'agit du pourcentage de toutes les I/O opérations de lecture sur le volume qui seront affectées par l'action.

Plage : min 0,1 %, maximum 100 %

- `readIOLatencyMilliseconds`— Quantité de latence injectée lors des I/O opérations de lecture. Il s'agit de la valeur de latence qui sera observée sur le pourcentage spécifié de la lecture I/O pendant l'expérience.

Portée : min 1 ms (io2) /10 ms (non-io2), max. 60 secondes

- `writeIOPercentage`— Pourcentage d' I/O opérations d'écriture pour lesquelles une latence sera injectée. Il s'agit du pourcentage de toutes les I/O opérations d'écriture sur le volume qui seront affectées par l'action.

Plage : min 0,1 %, maximum 100 %

- `writeIOLatencyMilliseconds`— Quantité de latence injectée lors des I/O opérations d'écriture. Il s'agit de la valeur de latence qui sera observée sur le pourcentage d'écriture spécifié I/O pendant l'expérience.

Portée : min 1 ms (io2) /10 ms (non-io2), 60 secondes maximum

- `duration`— Durée pendant laquelle la latence sera injectée sur la base du pourcentage I/O sélectionné.

Portée : minimum 1 seconde, maximum 12 heures

Surveillance de l'injection de latence

Vous pouvez surveiller l'impact des performances sur vos volumes de la manière suivante :

- Utilisez des mesures de latence moyenne CloudWatch pour obtenir la I/O latence moyenne par minute. Pour plus d'informations, voir [Surveillez vos volumes EBS à l'aide CloudWatch](#) de.
- Utilisez les statistiques de performances détaillées d'EBS disponibles via NVMe-CLI, CloudWatch agent et Prometheus pour obtenir une latence moyenne par seconde. I/O Les mesures détaillées

fournissent également des histogrammes de I/O latence que vous pouvez utiliser pour analyser la variance de latence de vos volumes. Pour plus d'informations, consultez les statistiques [de performances détaillées de NVMe](#).

- Utilisez [Vérifications de l'état des volumes Amazon EBS](#). Lorsque vous injectez de la I/O latence, l'état du volume passe à l'`warning` état.

Considérations

Lorsque vous utilisez l'injection de latence EBS, tenez compte des points suivants :

- L'injection de latence est prise en charge sur tous les types d'[Nitro-based instances](#), à l'exception de : P4d, P5, P5e, TRn2u, G6, G6f, Gr6, Gr6f, M8i,,, R8i,, i8GE et. M8i-flex C8i-flex R8i-flex Mac-m4pro Mac-m4
- Vous pouvez constater une variance allant jusqu'à 5 % entre la valeur de latence spécifiée dans l'expérience et la latence résultante observée.
- Si vous effectuez un très petit nombre d' I/O opérations, le pourcentage I/O indiqué dans les paramètres de l'action risque de ne pas correspondre au pourcentage réel d'opérations I/O touchées par l'action.

Pour exécuter une expérience d'injection de latence sur un volume Amazon EBS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez les volumes sur lesquels exécuter l'expérience et choisissez Actions, Tests de résilience, Injecter la I/O latence du volume.

La AWS Fault Injection Service console s'ouvre.

4. Dans la fenêtre Créer une expérience, sélectionnez le type d'expérience à exécuter : intermittent, croissant , soutenu ou décroissant.
5. Pour sélectionner le rôle IAM, choisissez Créer un nouveau rôle afin de créer un nouveau rôle qui AWS FIS sera utilisé pour mener les expériences en votre nom. Vous pouvez également choisir Utiliser un rôle IAM existant si vous avez déjà créé un rôle IAM avec les autorisations requises.
6. La section Estimation des prix vous donne une estimation du coût de l'exécution de l'expérience. Avec AWS FIS, vous êtes facturé par minute d'exécution d'une action, du début à la fin, en fonction du nombre de comptes cibles pour votre expérience.

7. Sélectionnez Start experiment (Démarrer une expérience).

Instantanés Amazon EBS

Vous pouvez sauvegarder les données de vos volumes Amazon EBS en créant des copies ponctuelles, appelées instantanés Amazon EBS. Un instantané est une sauvegarde incrémentielle, ce qui signifie que nous enregistrons uniquement les blocs sur le volume qui ont changé depuis votre instantané le plus récent. Cela réduit le temps nécessaire pour créer l'instantané, ainsi que les coûts de stockage en ne dupliquant pas les données.

Important

AWS ne sauvegarde pas automatiquement les données stockées sur vos volumes EBS. Pour garantir la résilience des données et la reprise après sinistre, il est de votre responsabilité de créer régulièrement des instantanés EBS, ou de configurer la création automatique d'instantanés à l'aide d'[Automatisez les sauvegardes avec Amazon Data Lifecycle Manager](#) or d'[AWS Backup](#).

Les instantanés sont stockés dans Amazon S3, dans des compartiments S3 auxquels vous ne pouvez pas accéder directement. Vous pouvez créer et gérer vos instantanés à l'aide de la console Amazon EC2 ou de l'API Amazon EC2. Vous ne pouvez pas accéder à vos instantanés via la console Amazon S3 ou l'API Amazon S3.

Les données des instantanés sont répliquées automatiquement dans toutes les zones de disponibilité de la région. Cela garantit une disponibilité et une durabilité élevées pour les données des instantanés, et vous permet de restaurer des volumes dans toutes les zones de disponibilité de cette région.

Chaque instantané contient toutes les informations nécessaires à la restauration de vos données (à partir du moment où l'instantané a été pris) sur un nouveau volume EBS. Lorsque vous créez un volume EBS à partir d'un instantané, au départ, le nouveau volume est donc une copie fidèle du volume qui a été utilisé pour créer l'instantané.

Pour plus d'informations, consultez la page produit des [Instantanés Amazon EBS](#).

Événements d'instantané

Vous pouvez suivre l'état de vos instantanés EBS via CloudWatch Events. Pour de plus amples informations, veuillez consulter [Événements d'instantané EBS](#).

Tarification des instantanés

Les frais pour vos instantanés sont basés sur la quantité de données stockées. Étant donné que les instantanés sont incrémentiels, la suppression d'un instantané risque de ne pas réduire vos coûts de stockage des données. Les données référencées exclusivement par un instantané sont supprimées lorsque cet instantané est supprimé, mais les données référencées par d'autres instantanés sont conservées. Pour plus d'informations, consultez [Volumes et instantanés Amazon Elastic Block Store](#) dans le Guide de l'utilisateur AWS Billing .

Table des matières

- [Comment fonctionnent les instantanés Amazon EBS](#)
- [Cycle de vie des instantanés Amazon EBS](#)
- [Restauration d'instantané rapide Amazon EBS](#)
- [Verrouillage d'instantanés Amazon EBS](#)
- [Bloquer l'accès public aux instantanés Amazon EBS](#)
- [Instantanés locaux Amazon EBS sur Outposts](#)
- [Instantanés locaux dans les zones locales](#)

Comment fonctionnent les instantanés Amazon EBS

Le premier instantané que vous créez à partir d'un volume est toujours un instantané complet. Il inclut tous les blocs de données écrits sur le volume au moment de la création de l'instantané. Les instantanés suivants du même volume sont des instantanés incrémentiels. Ils incluent uniquement les blocs de données modifiés et nouveaux écrits sur le volume depuis la création du dernier instantané

La taille d'un instantané complet est déterminée par la taille des données sauvegardées, et non par la taille du volume source. De même, les coûts de stockage associés à un instantané complet sont déterminés par la taille de l'instantané, et non par la taille du volume source. Par exemple, vous créez le premier instantané d'un volume Amazon EBS 200 GiB qui ne contient que 50 GiB de données. Il en résulte un instantané complet d'une taille de 50 GiB, et vous êtes facturé pour un stockage d'instantané de 50 GiB.

De même, la taille et les coûts de stockage d'un instantané incrémentiel sont déterminés par la taille des données écrites sur le volume depuis la création du cliché précédent. En reprenant l'exemple précédent, si vous créez un deuxième instantané du même 200 GiB volume après avoir modifié les

données et ajouté 20 GiB des données, la taille 10 GiB de la capture d'écran incrémentielle est 30 GiB maintenue. Vous êtes alors facturé pour ce stockage d'instantané supplémentaire de 30 GiB.

Pour plus d'informations sur la tarification des instantanés, consultez [Tarification Amazon EBS](#).

Important

Lorsque vous archivez un instantané incrémentiel, il est converti en instantané complet qui inclut tous les blocs écrits sur le volume au moment de la création de l'instantané. Il est ensuite déplacé vers le niveau Amazon EBS Snapshots Archive. Les instantanés du niveau d'archivage sont facturés à un tarif différent de celui des instantanés du niveau standard. Pour de plus amples informations, veuillez consulter [Tarification et facturation pour l'archivage des instantanés Amazon EBS](#).

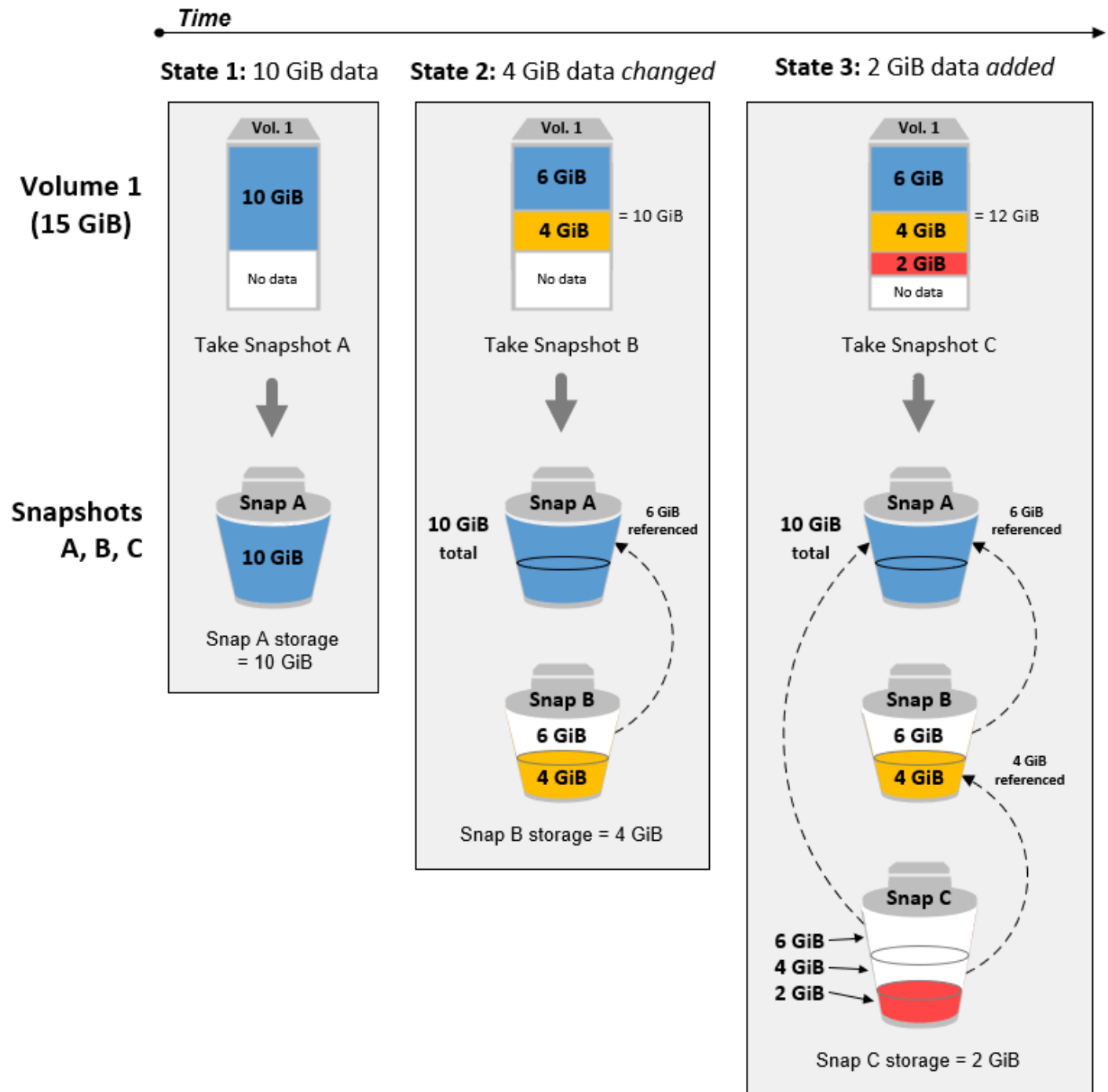
Les sections suivantes montrent comment un instantané EBS capture l'état d'un volume à un moment donné et dont des instantanés ultérieurs d'un volume modifié crée un historique de ces modifications.

Plusieurs instantanés d'un même volume

Le diagramme ci-dessous montre le Volume 1, d'une taille de 15 GiB, à trois moments différents. Un instantané de chacun de ces trois états du volume est pris. Le diagramme décrit spécifiquement les éléments suivants :

- Dans l'état State 1, le volume contient 10 GiB de données. Snap A est le premier instantané pris du volume. Snap A est un instantané complet et la totalité des 10 GiB de données est sauvegardée.
- Dans l'état State 2, le volume contient toujours 10 GiB de données, mais seuls 4 GiB ont changé depuis la prise de Snap A. Snap B est un instantané incrémentiel. Il ne doit sauvegarder que les 4 GiB qui ont changé. Les autres 6 GiB de données inchangées, qui sont déjà sauvegardées dans Snap A, sont référencées par Snap B au lieu d'être sauvegardées à nouveau. Ceci est indiqué par la flèche en pointillé.
- Dans l'état State 3, 2 GiB de données ont été ajoutés au volume, pour un total de 12 GiB, après que Snap B a été pris. Snap C est un instantané incrémentiel. Il ne doit sauvegarder que les 2 GiB qui ont été ajoutés après la prise de Snap B. Comme le montrent les flèches en pointillé, Snap C référence également les 4 GiB de données stockées dans Snap B et les 6 GiB de données stockées dans Snap A.

- L'espace de stockage total nécessaire pour les trois instantanés est de 16 GiB. Cela représente 10 Gio pour Snap A, 4 Gio et 2 Gio pour Snap C.



Instantanés incrémentiels de différents volumes

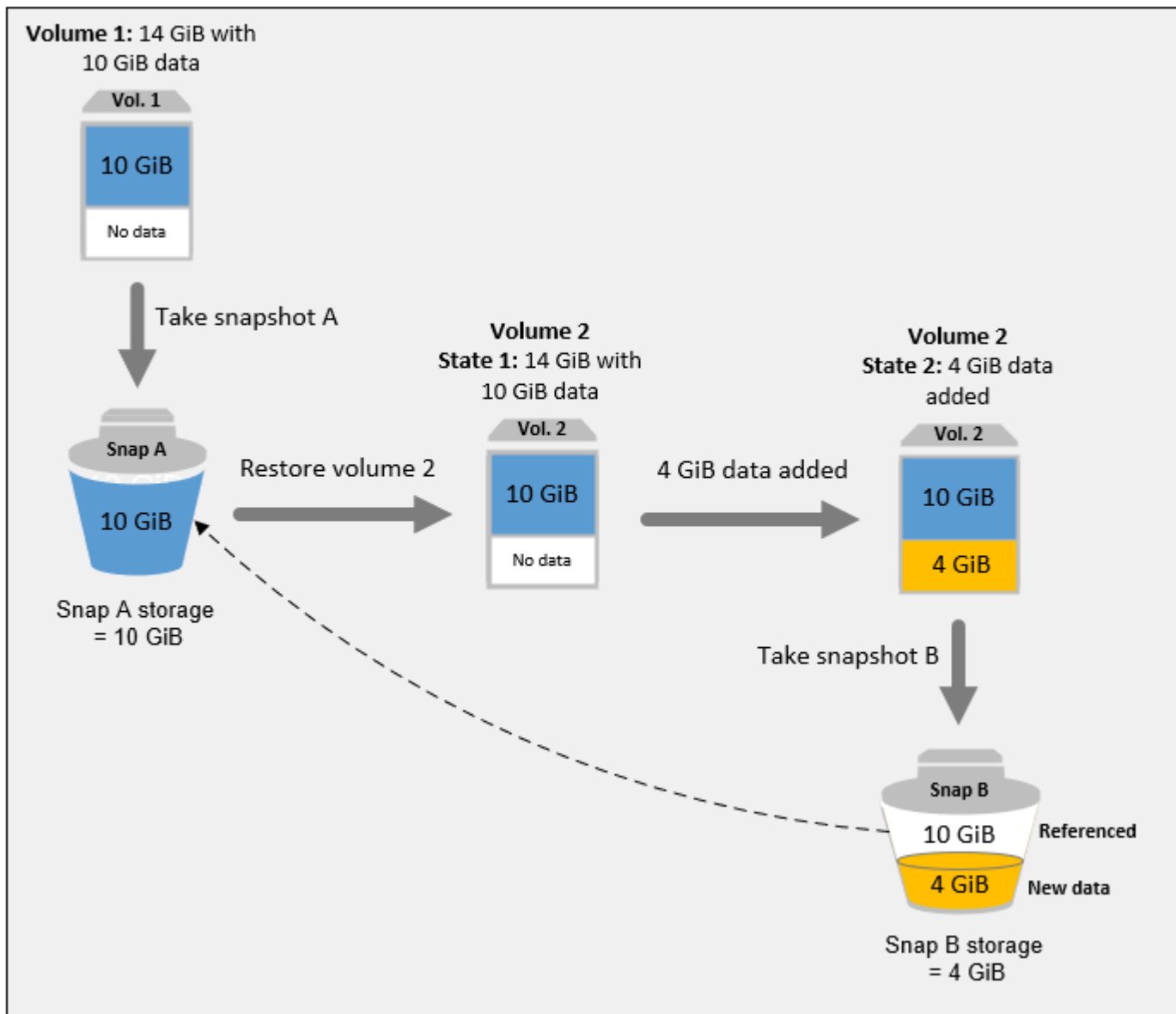
Le diagramme de cette section montre comment les instantanés incrémentiels peuvent être pris à partir de différents volumes.

1. Vol 1, qui a une taille de 14 GiB, contient 10 GiB de données. Snap A étant le premier instantané du volume, il s'agit d'un instantané complet et la totalité des 10 GiB de données est sauvegardée.
2. Vol 2 est créé à partir de Snap A, il s'agit donc d'une réplique exacte de Vol 1 au moment de la prise de l'instantané.
3. Au fil du temps, 4 GiB de données sont ajoutés au Vol 2 et la taille totale de ses données est de 14 GiB.
4. Snap B est pris de Vol 2. Pour Snap B, seuls les 4 GiB de données qui ont été ajoutées après la création du volume à partir de Snap A sont sauvegardées. Les autres 10 GiB de données non modifiées qui avaient déjà été copiés et stockés dans Snap A, sont référencés par Snap B au lieu d'être sauvegardée à nouveau.

Snap B est un instantané incrémentiel de Snap A, même s'il a été créé à partir d'un volume différent.

 Important

Le diagramme suppose que vous possédez Vol 1 et Snap A, et que Vol 2 est chiffré avec la même clé KMS que Vol 1. Si le vol 1 appartenait à un autre AWS compte et que ce compte prenait Snap A et le partageait avec vous, Snap B serait un instantané complet. Ou, si Vol 2 était chiffré avec une clé KMS différente de Vol 1, alors Snap B serait un instantané complet.



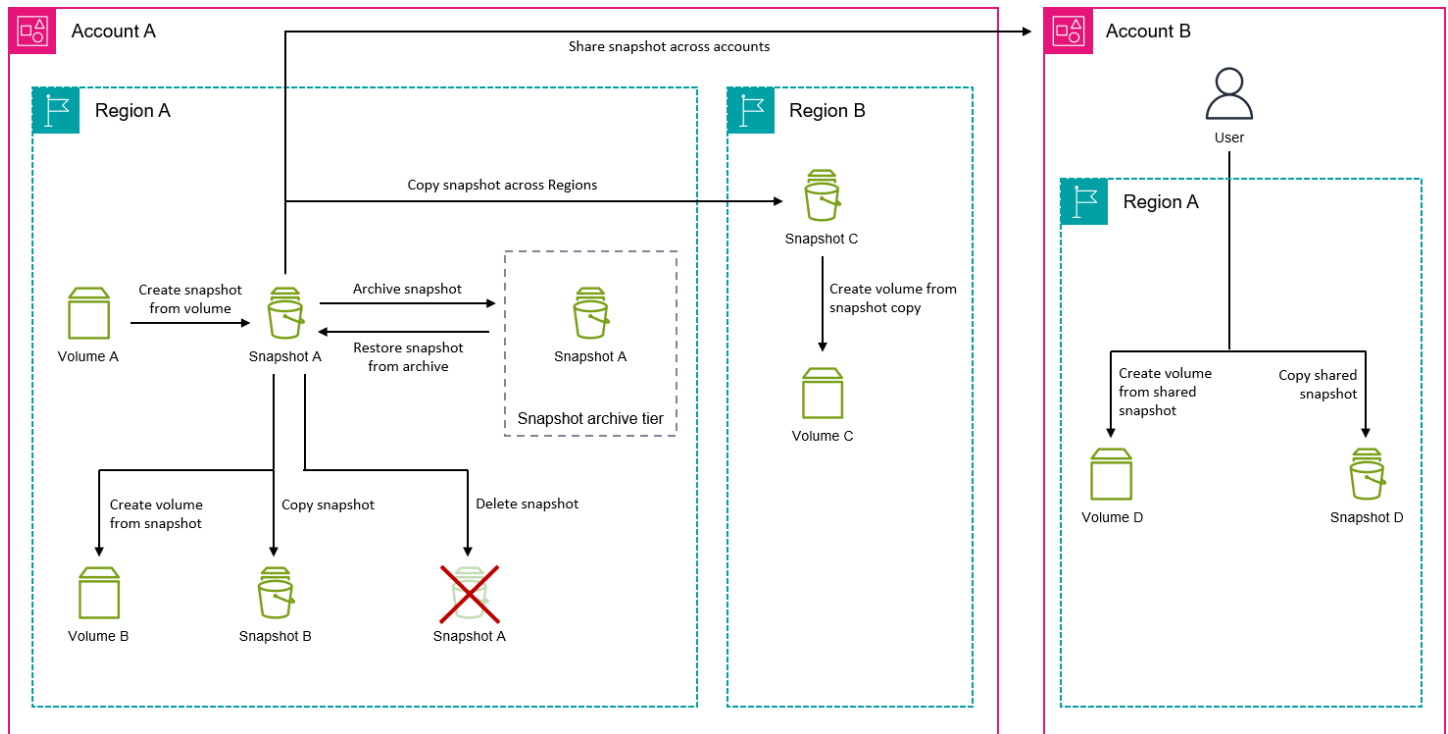
Pour plus d'informations sur la façon dont les données sont gérées lorsque vous supprimez un instantané, consultez [Supprimer un instantané Amazon EBS](#).

Cycle de vie des instantanés Amazon EBS

Le cycle de vie d'un instantané Amazon EBS commence par le processus de création. Vous créez des instantanés à partir de volumes Amazon EBS. Vous pouvez utiliser des instantanés pour restaurer de nouveaux volumes Amazon EBS. Vous pouvez créer des copies de clichés soit dans la même région, soit dans différentes régions. Vous pouvez partager des instantanés avec d'autres personnes Comptes AWS, en public ou en privé. Ces comptes peuvent restaurer des volumes à partir des instantanés partagés ou créer des copies des instantanés partagés sur leur propre compte.

Si vous n'avez pas besoin d'accéder immédiatement à un instantané, vous pouvez l'archiver pour économiser sur les coûts de stockage.

L'image suivante montre les actions que vous pouvez effectuer sur vos instantanés dans le cadre de leur cycle de vie.



Tâches

- [Créer des instantanés Amazon EBS](#)
- [Afficher les informations d'instantané Amazon EBS](#)
- [Copier un instantané Amazon EBS](#)
- [Partager un instantané Amazon EBS avec d'autres AWS comptes](#)
- [Archiver des instantanés Amazon EBS](#)
- [Supprimer un instantané Amazon EBS](#)

Créer des instantanés Amazon EBS

Vous pouvez créer un instantané Amazon EBS d'un volume Amazon EBS afin de créer une sauvegarde instantanée de ce volume. Vous pouvez soit créer des instantanés de volumes Amazon EBS individuels, soit créer des instantanés multi-volumes de l'ensemble ou d'un sous-ensemble des volumes attachés à une instance Amazon EC2.

La création d'instantanés est asynchrone. L'instantané est créé immédiatement, mais il reste dans pending cet état jusqu'à ce que toutes les données aient été transférées vers Amazon S3. Cette opération peut prendre plusieurs heures, en fonction du nombre de blocs modifiés sur le volume. Vous pouvez continuer à utiliser le volume pendant cette période sans affecter la capture d'écran. L'instantané inclut uniquement les données qui ont été écrites sur le volume au moment où le cliché a été demandé. Il n'inclut pas les données mises en cache par les applications ou le système d'exploitation.

 Tip

Pour vous assurer que les instantanés sont cohérents et complets, nous vous recommandons de suspendre les écritures sur le volume avant de créer l'instantané. Si vous ne pouvez pas suspendre les écritures sur le volume, nous vous recommandons de démonter le volume, depuis l'instance, avant de créer l'instantané. Vous pouvez remonter et reprendre les écritures une fois que l'instantané est entré dans l'état pending.

Si vous créez un instantané d'un volume qui sert de périphérique racine à une instance Amazon EC2, nous vous recommandons d'arrêter l'instance avant de prendre le snapshot.

Table des matières

- [Chiffrement des instantanés](#)
- [Destinations des instantanés](#)
- [Automatisation des instantanés](#)
- [Considérations relatives à la création d'instantanés](#)
- [Création d'un instantané d'un volume EBS](#)
- [Création d'instantanés EBS multivolumes à partir d'une instance EC2](#)

Chiffrement des instantanés

Un instantané obtient automatiquement le même état de chiffrement que le volume à partir duquel il a été créé. Les instantanés créés à partir de volumes non chiffrés ne sont pas chiffrés. Les instantanés créés à partir de volumes chiffrés sont automatiquement chiffrés à l'aide de la même clé KMS que le volume.

 Tip

Si vous devez créer un instantané chiffré à partir d'un volume non chiffré, créez d'abord l'instantané non chiffré du volume, puis créez une copie cryptée de cet instantané.

Destinations des instantanés

L'emplacement de la ressource source (volume ou instance) détermine l'endroit où vous pouvez créer des instantanés.

- Si la ressource source se trouve dans une région, vous devez créer des instantanés dans la même région que la ressource source.
- Si la ressource source se trouve dans une zone locale, vous pouvez créer des instantanés dans la même zone locale ou dans sa région parente. Pour de plus amples informations, veuillez consulter [Instantanés locaux dans les zones locales](#).
- Si la ressource source se trouve sur une Outpost, vous pouvez créer des instantanés sur la même région Outpost ou dans sa région mère. Pour de plus amples informations, veuillez consulter [Instantanés locaux Amazon EBS sur Outposts](#).

Automatisation des instantanés

Vous pouvez automatiser la création d'instantanés à l'aide [d'Amazon Data Lifecycle Manager](#) et [AWS Backup](#).

Considérations relatives à la création d'instantanés

- Nous vous recommandons de ne pas créer d'instantanés des volumes attachés à des instances Amazon EC2 mises en veille prolongée ou activées pour la mise en veille prolongée. Pour plus d'informations, consultez [Comment fonctionne la mise en veille prolongée des instances Amazon EC2](#).
- Bien que vous puissiez prendre un instantané d'un volume alors que l'pendingétat d'un instantané précédent de ce volume est en cours, le fait de disposer de plusieurs instantanés dans l'pendingétat d'un même volume peut entraîner une réduction des performances du volume jusqu'à ce que les instantanés soient terminés.
- Le nombre d'instantanés que vous pouvez avoir dans l'pendingétat est limité et le nombre d'instantanés simultanés que vous pouvez demander par type de volume. Pour plus d'informations,

consultez la section [Quotas pour Amazon EBS](#). Si vous dépassez l'un de ces quotas, attendez que les instantanés actuels soient terminés, puis réessayez.

Création d'un instantané d'un volume EBS

Vous pouvez créer un instantané unique d'un seul volume. Vous pouvez également automatiser la création d'instantanés en utilisant [Amazon Data Lifecycle Manager](#) ou [AWS Backup](#). Pour créer des instantanés de tous les volumes d'une instance EC2, utilisez des instantanés [multi-volumes](#).

Console

Pour créer un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés), Create snapshot (Créer un instantané).
3. Pour Type de ressource, choisissez Volume.
4. Pour Volume ID (ID de volume), sélectionnez le volume à partir duquel créer l'instantané. Le champ Chiffrement indique le volume et l'état de chiffrement de l'instantané qui en résulte. Il ne peut pas être modifié.
5. (Facultatif) Dans le champ Description, entrez une brève description de la capture d'écran.
6. Si le volume se trouve dans une zone locale Outpost ou dans une zone locale, le champ Destination du snapshot apparaît. Effectuez l'une des actions suivantes :
 - Si le volume se trouve dans une zone locale, choisissez Zone locale pour créer le cliché dans la même zone locale, ou choisissez AWS Région pour créer l'instantané dans la région parent de la zone locale.
 - Si le volume se trouve sur un Outpost AWS Outpost, choisissez de créer l'instantané sur le même Outpost ou choisissez AWS Région pour créer l'instantané dans la région parent du Outpost.

Note

Si le volume se trouve dans une région, la destination du snapshot n'apparaît pas. L'instantané est automatiquement créé dans la même région que le volume.

7. (Facultatif) Pour attribuer des balises personnalisées à l'instantané, dans la section Balises, choisissez Ajouter une balise, puis entrez la paire clé-valeur. Vous pouvez ajouter jusqu'à 50 balises.
8. Choisissez Créer un instantané.

AWS CLI

Pour créer un instantané

Utilisez la commande [create-snapshot](#).

```
aws ec2 create-snapshot \  
  --volume-id vol-01234567890abcdef \  
  --description "Snapshot of the root volume for i-1234567890abcdef0"
```

PowerShell

Pour créer un instantané

Utilisez l'applet de commande [New-EC2Snapshot](#).

```
New-EC2Snapshot `  
  -VolumeId vol-01234567890abcdef `  
  -Description "Snapshot of the root volume for i-1234567890abcdef0"
```

Création d'instantanés EBS multivolumes à partir d'une instance EC2

Par défaut, lorsque vous créez des instantanés multi-volumes à partir d'une instance Amazon EC2, Amazon EBS crée des instantanés de tous les volumes Amazon EBS attachés à l'instance. Vous pouvez toutefois choisir d'exclure le volume racine ou des volumes de données spécifiques si nécessaire.

Tip

Nous vous recommandons de baliser vos instantanés multivolumes afin de les identifier et de les gérer collectivement en toute simplicité. Vous pouvez également copier les balises des volumes sources vers les instantanés correspondants afin de définir les métadonnées des

instantanés, telles que les politiques d'accès, les informations relatives aux pièces jointes et la répartition des coûts, en fonction du volume source.

Considérations relatives aux instantanés multivolumes

- Si toutes les captures d'écran sont effectuées correctement, un `createSnapshots` CloudWatch événement dont le résultat `succeeded` est envoyé à votre AWS compte. Si l'un des instantanés de l'ensemble d'instantanés multivolumes échoue, tous les autres instantanés passent à l'état `error` et un `createSnapshots` CloudWatch événement dont le résultat `failed` est envoyé à votre compte. Pour de plus amples informations, veuillez consulter [Créer des instantanés \(createSnapshots\)](#).
- Multi-volume les instantanés prennent en charge jusqu'à 128 volumes Amazon EBS attachés à une instance, y compris le volume racine et jusqu'à 127 volumes de données.
- Chaque instantané de l'ensemble d'instantanés multivolumes est un instantané individuel qui peut être utilisé de la même manière et qui prend en charge les mêmes fonctionnalités qu'un instantané individuel.
- Vous pouvez prendre des instantanés cohérents avec les applications de tous les volumes Amazon EBS attachés à une instance Windows Amazon EC2 à l'aide de documents de commande. [AWS Systems Manager](#)

Console

Pour créer des instantanés multivolumes

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés), Create snapshot (Créer un instantané).
3. Pour Resource type (Type de ressource), choisissez Instance.
4. (Facultatif) Pour Description, saisissez une brève description pour les instantanés. Cette description s'applique à tous les instantanés.
5. Si l'instance se trouve dans une zone locale Outpost ou dans une zone locale, le champ Destination du snapshot apparaît. Effectuez l'une des actions suivantes :

- Si l'instance se trouve dans une zone locale, choisissez **Zone locale** pour créer les instantanés dans la même zone locale, ou choisissez **AWS Région** pour créer les instantanés dans la région parent de la zone locale.
- Si l'instance se trouve sur un Outpost, choisissez **AWS Outpost**, pour créer les instantanés sur la même Outpost, ou choisissez **AWS Région** pour créer les instantanés dans la région parent du Outpost.

 Note

Si l'instance se trouve dans une région, la destination du snapshot n'apparaît pas. L'instantané est automatiquement créé dans la même région que l'instance.

6. (Facultatif) Pour exclure le volume racine de l'instance, sélectionnez **Exclure le volume racine**.
7. (Facultatif) Pour exclure des volumes de données, sélectionnez **Exclure des volumes de données spécifiques**. La section **Attached data volumes** (Volumes de données attachés) répertorie tous les volumes de données qui sont actuellement attachés à l'instance sélectionnée.

Sélectionnez les volumes de données à exclure. Seuls les volumes qui ne sont pas sélectionnés seront inclus dans l'ensemble d'instantanés multi-volumes.

8. (Facultatif) Pour copier automatiquement les balises des volumes source vers les instantanés correspondants, pour **Copier les balises depuis le volume source**, sélectionnez **Copier les balises**.
9. (Facultatif) Pour attribuer des balises personnalisées supplémentaires aux instantanés, dans la section **Tags**, choisissez **Ajouter une balise**, puis entrez la paire clé-valeur. Vous pouvez ajouter jusqu'à 50 balises.
10. Choisissez **Créer un instantané**.

AWS CLI

Pour créer des instantanés multivolumes

Utilisez la commande [create-snapshots](#).

```
aws ec2 create-snapshots \
```

```
--instance-specification InstanceId=i-1234567890abcdef0 \  
--description "from a multi-volume snapshot of i-1234567890abcdef0"
```

Pour exclure le volume racine, ajoutez ce qui suit à l'`--instance-specification`option.

```
ExcludeBootVolume=true
```

Pour exclure un volume de données, ajoutez ce qui suit à l'`--instance-specification`option.

```
ExcludeDataVolumeIds=vol-01234567890abcdef
```

PowerShell

Pour créer des instantanés multivolumes

Utilisez l'applet de commande [New-EC2SnapshotBatch](#).

```
New-EC2SnapshotBatch `   
-InstanceSpecification_InstanceId i-1234567890abcdef0 `   
-Description "from a multi-volume snapshot of i-1234567890abcdef0"
```

Pour exclure le volume racine, ajoutez le paramètre suivant.

```
-InstanceSpecification_ExcludeBootVolume $true
```

Pour exclure des volumes de données, ajoutez le paramètre suivant.

```
-InstanceSpecification_ExcludeDataVolumes "vol-01234567890abcdef"
```

Afficher les informations d'instantané Amazon EBS

Vous pouvez afficher des informations détaillées sur vos instantanés.

Console

Pour afficher les informations relatives aux instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Pour afficher uniquement les instantanés que vous possédez, dans le coin supérieur gauche de l'écran, choisissez Owned by me (M'appartenant). Vous pouvez également filtrer la liste des instantanés en utilisant des identifications et d'autres attributs d'instantanés. Dans le champ Filter (Filtrer), sélectionnez le champ attribut, puis sélectionnez ou saisissez la valeur de l'attribut. Par exemple, pour afficher uniquement des instantanés chiffrés, sélectionnez Encryption (Chiffrement), puis saisissez `true`.
4. Pour afficher des informations supplémentaires sur un instantané spécifique, choisissez son ID dans la liste.

 Note

Le champ Taille complète de l'instantané indique la taille totale de l'instantané, en octets. Il ne s'agit pas de la taille incrémentielle de l'instantané. Il représente plutôt la taille de tous les blocs qui ont été écrits sur le volume source au moment de la création de l'instantané.

Le champ Taille du volume indique la taille du volume EBS qui sera créé à partir de l'instantané si aucune autre taille n'est spécifiée.

AWS CLI

Pour afficher les informations relatives aux instantanés

Utilisez la commande [describe-snapshots](#).

Exemple Exemple 1 : filtre basé sur les balises

L'exemple suivant décrit les instantanés avec la balise Stack=Production.

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Exemple Exemple 2 : filtre basé sur le volume

L'exemple suivant décrit les instantanés créés à partir du volume spécifié.

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```


Exemple Exemple 3 : filtre basé sur l'ancienneté des instantanés

Vous pouvez utiliser JMESPath pour filtrer les résultats à l'aide d'expressions. Par exemple, la commande suivante affiche les ID de tous les instantanés créés par votre compte avant la date spécifiée. Si vous ne spécifiez pas le propriétaire, les résultats incluent tous les instantanés publics.

```
aws ec2 describe-snapshots \  
  --filters Name=owner-id,Values=123456789012 \  
  --query "Snapshots[?(StartTime<='2024-03-31')].[SnapshotId]" \  
  --output text
```

La commande suivante affiche les ID de tous les instantanés créés dans la plage de dates spécifiée.

```
aws ec2 describe-snapshots \  
  --filters Name=owner-id,Values=123456789012 \  
  --query "Snapshots[?(StartTime>='2024-01-01') && (StartTime<='2024-12-31')].  
[SnapshotId]" \  
  --output text
```

PowerShell

Pour afficher les informations relatives aux instantanés

Utilisez l'applet de commande [Get-EC2Snapshot](#).

Exemple 1 : Décrire un instantané

L'exemple suivant décrit l'instantané spécifié.

```
Get-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

Exemple 2 : filtre basé sur le volume

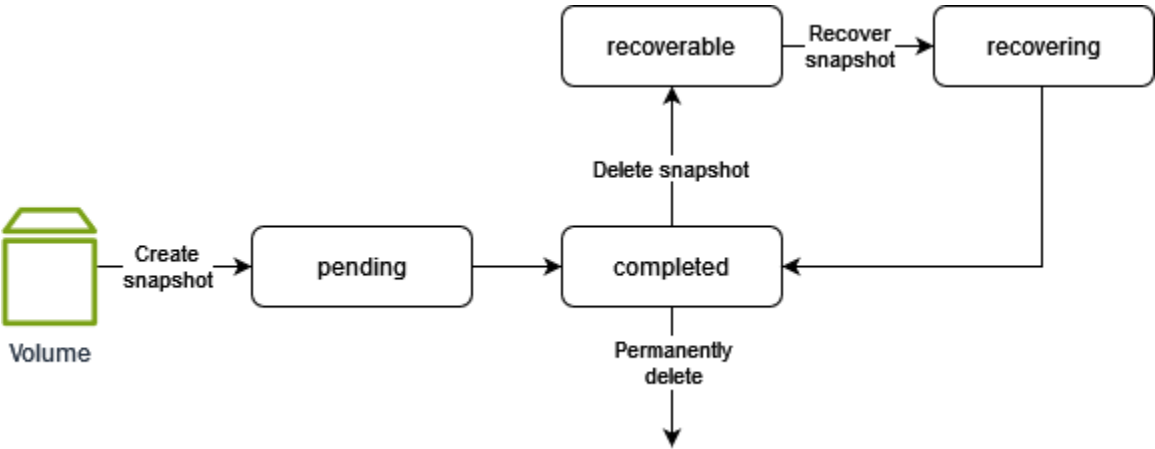
L'exemple suivant décrit les instantanés créés à partir du volume spécifié.

```
Get-EC2Snapshot `  
  -Filter @{Name="volume-id"; Values="vol-01234567890abcdef"}
```

États des instantanés

Un instantané Amazon EBS passe par différents états entre le moment où il est créé et sa suppression définitive.

L'illustration suivante montre les transitions entre les états de capture d'écran. Lorsque vous créez un instantané, il entre dans l'`pending` état. Une fois que l'instantané est prêt à être utilisé, il passe à l'`completed` état. Lorsque vous avez décidé que vous n'avez plus besoin d'un instantané, vous pouvez le supprimer. Si vous supprimez un instantané qui correspond à une règle de conservation de la corbeille, il est conservé dans la corbeille et il entre dans `recoverable` cet état. Si vous récupérez un instantané depuis la corbeille, il entre dans l'`recovering` état, puis dans l'`completed` état. Dans le cas contraire, il est définitivement supprimé.



Le tableau suivant récapitule les états des instantanés.

Statut	Description
pending	Le processus de création d'instantanés est toujours en cours. Un instantané ne peut pas être utilisé tant qu'il est dans pending cet état.
completed	Le processus de création de l'instantané est terminé et le cliché est prêt à être utilisé.
recoverable	L'instantané se trouve actuellement dans la corbeille. Pour utiliser l'instantané, vous devez d'abord le récupérer depuis la corbeille.

Statut	Description
recovering	L'instantané est en cours de restauration depuis la corbeille. Une fois que l'instantané a été restauré, il passe à l' <code>completed</code> état et est prêt à être utilisé.
error	Le processus de création d'un instantané a échoué. Un instantané ne peut pas être utilisé s'il est dans <code>error</code> cet état.

Copier un instantané Amazon EBS

Une fois que vous avez créé un instantané et qu'il a atteint `completed` cet état, vous pouvez en créer une copie. La copie instantanée est une copie exacte de l'original, mais elle possède un identifiant de ressource unique. Vous pouvez copier des instantanés qui vous appartiennent et des instantanés que vous partagez avec vous, en privé ou en public. Il se peut que vous deviez copier un instantané pour les cas d'utilisation suivants :

- Expansion géographique — Vous devez lancer vos applications dans une nouvelle région.
- Migration : vous devez déplacer une application vers une nouvelle destination, afin d'améliorer la disponibilité ou de minimiser les coûts.
- Reprise après sinistre : vous devez sauvegarder vos données et vos journaux dans des régions secondaires à des fins de redondance des données.
- Chiffrement : vous devez chiffrer un instantané précédemment non chiffré ou rechiffrer un instantané chiffré à l'aide d'une autre clé KMS.
- Copier un instantané partagé : vous devez copier un instantané partagé avec vous.
- Exigences en matière de conservation et d'audit des données : vous devez copier des instantanés chiffrés d'un AWS compte à un autre afin de préserver les données à des fins d'audit ou de conservation des données. L'utilisation d'un autre compte vous protège si votre AWS compte principal est compromis.

Pour copier des instantanés multivolumes, identifiez tous les instantanés qui font partie de cet ensemble à l'aide des balises que vous avez attribuées lors de la création, puis copiez-les individuellement.

Pour plus d'informations sur la copie d'un instantané Amazon RDS, consultez [Copie d'un instantané de base de données](#) dans le Amazon RDS Guide de l'utilisateur.

Tarification

Pour obtenir des informations sur les tarifs relatifs à la copie d'instantanés, consultez la page Tarification [d'Amazon EBS](#).

Table des matières

- [Considérations relatives à la copie d'instantanés](#)
- [Destinations pour les copies instantanées](#)
- [Copie d'instantané incrémentielle](#)
- [Time-based copies pour les instantanés et les AMI Amazon EBS EBS-backed](#)
- [Chiffrement et copie d'instantanés](#)
- [Copie d'un instantané](#)

Considérations relatives à la copie d'instantanés

- Vous pouvez copier AWS Marketplace des instantanés de VM Import/Export et de Storage Gateway, mais vous devez vérifier que les instantanés sont pris en charge dans la région de destination.
- Il existe une limite de demandes 20 simultanées de copie de snapshots par destination. Si vous dépassez ce quota, vous recevez une erreur ResourceLimitExceeded. Si cette erreur s'affiche, attendez qu'une ou plusieurs des demandes de copie soient terminées avant d'effectuer une nouvelle demande de copie d'instantané.
- User-defined les balises ne sont pas copiées de l'instantané source vers la copie de l'instantané. Vous pouvez ajouter des balises définies par l'utilisateur pendant ou après l'opération de copie.
- Les instantanés créés par une opération de copie d'instantané ont un ID de volume arbitraire, tel que vol-ffff ou vol-fffffffffff. Ces ID de volume arbitraires ne doivent être utilisés en aucun cas.
- Resource-level les autorisations spécifiées pour l'opération de copie du cliché peuvent s'appliquer à la copie du cliché et à l'instantané source. Pour un exemple, voir [Exemple : copie d'instantanés](#).
- Si vous copiez un instantané qui est activé pour la restauration rapide des instantanés, la copie des instantanés n'est pas automatiquement activée pour la restauration rapide des instantanés. Vous devez activer explicitement la restauration rapide des instantanés pour la copie des instantanés.

- Si vous copiez un instantané et le chiffrez dans une nouvelle clé KMS, une copie complète (non incrémentielle) est créée. Cela entraîne des coûts de stockage supplémentaires.
- Si vous copiez un instantané dans une nouvelle région, une copie complète (non incrémentielle) est créée. Cela entraîne des coûts de stockage supplémentaires.
- Si vous utilisez des transferts de données externes ou interrégionaux, des [frais de transfert de données](#) EC2 supplémentaires s'appliqueront. Si vous supprimez des instantanés après le lancement, les données qui ont déjà été transférées vous seront toujours facturées.

Destinations pour les copies instantanées

L'emplacement de l'instantané source détermine si vous pouvez le copier ou non.

- Si l'instantané source se trouve dans une région, vous pouvez le copier dans cette région, dans une autre région, dans une zone Outpost associée à cette région ou dans une zone locale de cette région.
- Si l'instantané source se trouve dans une zone locale, vous pouvez le copier dans la même zone locale, dans une autre zone locale du même groupe de zones ou dans la région parent de cette zone locale.
- Si l'instantané source se trouve sur un Outpost, vous ne pouvez pas le copier.

Copie d'instantané incrémentielle

Les opérations de copie de snapshots effectuées au sein d'un même compte et d'une même région à l'aide de la même clé KMS sont toujours des copies incrémentielles. Toutefois, si vous chiffrez la copie de l'instantané à l'aide d'une autre clé KMS, il s'agit d'une copie complète.

Lorsque vous copiez un instantané entre des régions ou des comptes, la copie est une copie incrémentielle si les conditions suivantes sont remplies :

- L'instantané a été préalablement copié dans la région ou le compte de destination.
- La dernière copie d'instantané existe toujours dans la région ou le compte de destination.
- La copie instantanée la plus récente n'a pas été archivée.
- Toutes les copies de l'instantané dans la région ou dans le compte de destination sont soit non chiffrées, soit chiffrées avec la même clé KMS.

 Tip

Nous vous recommandons d'étiqueter vos copies instantanées avec l'ID du volume et l'heure de création afin de pouvoir suivre la copie instantanée la plus récente d'un volume dans la région ou le compte de destination.

Pour savoir si vos copies d'instantanés sont incrémentielles, consultez l'événement [CopySnapshot](#) CloudWatch .

Time-based copies pour les instantanés et les AMI Amazon EBS EBS-backed

Time-based les copies peuvent vous aider à répondre aux exigences de conformité ou commerciales en matière de réplication des données en garantissant que vos instantanés EBS et vos EBS-backed AMI sont copiés, au sein des AWS régions et entre elles, dans un délai spécifié. Time-based les copies peuvent également aider les administrateurs de sauvegarde à répondre à des exigences strictes en matière de reprise après sinistre (objectifs de point de restauration et objectifs de temps de restauration), et elles améliorent l'agilité du développement en garantissant des temps de copie prévisibles pour les snapshots et les EBS-backed AMI.

Avec les opérations de capture d'écran et de copie d' EBS-backed AMI basées sur le temps, vous spécifiez une durée de réalisation, comprise entre 15 minutes et 48 heures, pendant laquelle la copie doit être terminée. La durée de réalisation doit être spécifiée par tranches de 15 minutes.

Rubriques

- [Quotas](#)
- [Déterminez votre durée de réalisation](#)
- [Considérations](#)
- [Contrôle](#)
- [Tarification et facturation](#)

Quotas

Les quotas suivants s'appliquent aux opérations de capture d'écran et de copie d' EBS-backed AMI basées sur le temps :

Quota	Description	Valeur du quota	Ajustable
Quota de débit pour les opérations de copie instantanée	<p>Débit maximal pouvant être atteint par une seule opération de copie d'instantané basée sur le temps.</p> <div>  Note Pour les opérations de copie d'AMI, le quota s'applique à chaque instantané individuel associé à l'AMI. </div>	500 MiB/s	Non
Quota de débit cumulé pour la copie de clichés	<p>Débit cumulé maximal pouvant être atteint par des opérations simultanées de copie d'instantanés basées sur le temps entre une région source et une région de destination.</p> <div>  Note Pour les opérations de copie d'AMI, chaque </div>	2 000 MiB/s	Oui

Quota	Description	Valeur du quota	Ajustable
	instantané individuel associé à l'AMI est pris en compte dans le quota.		

Lorsque vous lancez une opération de copie d'instantané basée sur le temps, vous spécifiez une durée d'exécution. Le débit utilisé par la demande est déterminé par la taille des données de capture instantanée et la durée d'exécution demandée. Par exemple, si vous copiez un instantané contenant 225 000 MiB (0,214 TiB) de données et que vous demandez une durée de réalisation de 15 minutes, le débit est de 250 MiB/s ($225\,000 \text{ MiB} \div 15 \text{ minutes} = 250$). MiB/s

Lorsque vous lancez une opération de copie d'AMI basée sur le temps, la durée d'exécution que vous spécifiez s'applique à chaque instantané associé à l'AMI. Étant donné que chaque instantané peut avoir une taille différente, chaque instantané est copié à un débit différent afin de garantir que tous les instantanés sont copiés dans les délais impartis. Supposons, par exemple, que vous disposiez d'une AMI avec les instantanés associés suivants :

- Instantané 1 : 200 000 MiB
- Instantané 2 : 500 000 MiB
- Instantané 3 : 450 000 MiB

Si vous lancez une copie basée sur le temps pour cette AMI et que vous spécifiez une durée de traitement de 60 minutes, la demande utilise le débit suivant :

- Instantané 1 : 55,56 MiB/s ($200\,000 \text{ MiB} \div 60 \text{ minutes} = 55,56$) MiB/s
- Instantané 2 : 138,89 MiB/s ($500\,000 \text{ MiB} \div 60 \text{ minutes} = 138,89$) MiB/s
- Instantané 3 : 125 MiB/s ($450\,000 \text{ MiB} \div 60 \text{ minutes} = 125$) MiB/s

Cela signifie que la demande utilise 319,45 % MiB/s de votre quota de débit de copie de snapshot cumulé pour s'assurer que la copie est terminée en 60 minutes.

Si vous lancez une demande de copie d'instantané ou d' EBS-backed AMI basée sur le temps et que votre quota de débit de copie de cliché cumulé disponible est le suivant :

- supérieur ou égal au débit requis, la copie est terminée dans le délai de réalisation demandé.
- inférieur au débit requis mais supérieur à zéro, la demande aboutit mais elle prendra plus de temps que vous ne l'avez demandé. La copie est terminée en utilisant votre quota de débit disponible.
- zéro (quota atteint), la demande échoue.

Déterminez votre durée de réalisation

La durée d'exécution minimale que vous pouvez demander pour une opération de copie d'un instantané ou d'une EBS-backed AMI basée sur le temps est de 15 minutes, et la durée maximale de réalisation que vous pouvez demander est de 48 heures. La durée de réalisation doit être spécifiée par tranches de 15 minutes.

Opérations simultanées de copie de snapshots basées sur le temps

Vous pouvez effectuer des opérations simultanées de copie d'instantanés basées sur le temps entre les mêmes régions source et de destination, à condition que le débit combiné de toutes les opérations simultanées ne dépasse pas votre quota de débit cumulé de copies de clichés (2 000 MiB/s par défaut).

Pour déterminer si vous pouvez atteindre la durée de réalisation requise pour vos instantanés existants, divisez la taille combinée de tous vos instantanés par la durée de réalisation requise afin de déterminer le débit requis.

Tip

Si vous ne connaissez pas la taille exacte des données de vos instantanés, vous pouvez utiliser la taille complète de l'instantané comme proxy. Pour obtenir la taille complète de l'instantané, utilisez la commande [describe-snapshots](#) AWS CLI .

```
required throughput rate = combined snapshot size ÷ required completion duration
```

Si le débit requis est inférieur à votre quota de débit cumulé pour la copie de snapshots, vous pouvez atteindre la durée d'exécution requise. Si le débit requis est supérieur à votre quota de débit cumulé

pour la copie de clichés, nous vous recommandons de demander une augmentation de quota supérieure d'au moins 10 % au débit requis.

 Tip

La console Amazon EC2 fournit un calculateur que vous pouvez utiliser pour vérifier la quantité de données de snapshot que vous avez copiées entre deux régions au cours d'une période donnée, ainsi que la durée de réalisation minimale que vous pouvez atteindre pour cette quantité de données, sur la base d'un quota de débit de copie de snapshot cumulé spécifique. Le calculateur utilise la `SnapshotCopyBytesTransferred` CloudWatch métrique pour calculer les données copiées entre deux régions au cours d'une période. Pour ouvrir la calculatrice, dans le panneau de navigation de la console Amazon EC2, sélectionnez **Instantanés**, puis choisissez **Actions**, **Lancer le calculateur de durée de copie**. Le calculateur de durée de copie des instantanés n'est pas pris en charge avec AWS Outposts les zones locales et les zones de longueur d'onde.

Opérations de copie d'instantanés individuelles basées sur le temps

Vous pouvez calculer la durée minimale d'achèvement d'une opération de copie de cliché individuelle basée sur le temps en divisant la taille des données de cliché par le quota de débit de l'opération de copie de cliché (500 MiB/s).

 Tip

Si vous ne connaissez pas la taille exacte des données de vos instantanés, vous pouvez utiliser la taille complète de l'instantané comme proxy. Pour obtenir la taille complète de l'instantané, utilisez la commande [describe-snapshots](#) AWS CLI .

```
minimum completion duration = Max(15 minutes, (snapshot data size ÷ 500 MiB/s))
```

Par exemple, la durée minimale de réalisation d'un instantané contenant 900 000 Mo de données est de 30 minutes.

```
minimum completion duration = Max(15 minutes, (900,000 MiB ÷ 500 MiB/s))
```

```
= Max(15 minutes, 30 minutes)
= 30 minutes
```

Time-based Opérations de copie AMI

Lorsque vous lancez une opération de copie d'AMI basée sur le temps pour une EBS-backed AMI à laquelle un seul instantané est associé, elle se comporte de la même manière qu'une opération de copie d'instantané basée sur le temps individuelle, et les mêmes limites de débit s'appliquent.

Lorsque vous lancez une opération de copie d'AMI basée sur le temps pour une EBS-backed AMI à laquelle plusieurs instantanés sont associés, elle se comporte de la même manière que les opérations simultanées de copie d'instantanés basées sur le temps et les mêmes limites de débit s'appliquent. Chaque instantané associé donne lieu à une demande de copie d'instantané distincte, chacune de ces demandes contribuant à votre quota de débit cumulé de copies d'instantanés. La durée d'exécution que vous spécifiez s'applique à chaque instantané associé.

Considérations

- Vous pouvez lancer des opérations de copie d'instantanés et d' EBS-backed AMI basées sur le temps lorsque vous copiez des instantanés au sein d'une même région ou lorsque vous copiez des instantanés entre régions.
- Si vous lancez deux opérations de copie basées sur le temps pour le même snapshot ou AMI, la durée de fin de la deuxième opération de copie ne commence qu'une fois la première opération de copie terminée.
- Time-based les opérations de copie et le calculateur de durée de copie des instantanés ne sont pas pris en charge avec AWS Outposts les zones locales et les zones de longueur d'onde.

Contrôle

Vous pouvez suivre la progression des opérations de copie des instantanés et des EBS-backed AMI basées sur le temps à l'aide de la console Amazon EC2 et du AWS CLI. Dans la console, sélectionnez l'instantané, puis, dans l'onglet Détails, inspectez le champ Progression. Avec le AWS CLI, inspectez l'élément Progress de sortie dans la réponse de [commande describe-snapshots](#).

Vous pouvez vérifier si une opération de copie d'un instantané ou d'une EBS-backed AMI basée sur le temps s'est terminée dans le délai demandé en vérifiant la différence entre les heures de début et de fin dans la console ou StartTime CompletionTime dans la describe-snapshots réponse.

Vous pouvez également utiliser l' EventBridge événement copySnapshot Amazon pour suivre le résultat des opérations de copie basées sur le temps. L'événement indique si l'opération s'est terminée et si la durée de réalisation demandée a été respectée. Si la durée de réalisation n'a pas été respectée, l'événement inclut plus d'informations sur la cause. Pour de plus amples informations, veuillez consulter [Événements d'instantané EBS](#).

Tarification et facturation

Note

Comme pour les opérations de copie de clichés standard, si vous copiez un instantané vers une nouvelle région, une copie complète (non incrémentielle) est créée, ce qui entraîne des coûts de stockage supplémentaires. Les copies suivantes du même instantané sont incrémentielles. En outre, si vous utilisez des transferts de données externes ou entre régions, des frais de transfert de données Amazon EC2 supplémentaires s'appliqueront.

Des frais supplémentaires s'appliquent pour les opérations de capture d'écran basées sur la durée et de copie d' EBS-backed AMI. Time-based les opérations de copie sont facturées à un tarif basé sur la durée de réalisation demandée, par Go de données de capture copiées. Les taux fixes sont les suivants :

Note

La durée de réalisation doit être spécifiée par tranches de 15 minutes. La durée minimale de réalisation est de 15 minutes et la durée maximale de 48 heures.

- 15 minutes — 0,020\$ par Go de données
- 30 minutes et 45 minutes — 0,018\$ par Go de données
- 1 heure à 1 heure 45 minutes — 0,016\$ par Go de données
- 2 heures à 3 heures 45 minutes — 0,014\$ par GiB de données
- 4 heures à 7 heures 45 minutes — 0,012\$ par GiB de données
- 8 heures à 15 heures 45 minutes — 0,010\$ par GiB de données
- 16 heures ou plus — 0,005\$ par GiB de données

Par exemple, si vous copiez un instantané contenant 3 000 Go de données avec une durée de réalisation de 8 heures, vous êtes facturé 30\$ (0,010\$ x 3 000 GiB).

Si vous lancez une opération de copie basée sur le temps, mais que la durée de réalisation requise n'est pas atteinte parce que vous dépassez un quota, vous êtes facturé sur la base de la durée de réalisation réelle au lieu de la durée de réalisation demandée. Par exemple, si vous demandez une durée de réalisation d'une heure, mais que l'opération se termine en 2 heures, vous êtes facturé sur la base du tarif correspondant à la durée de réalisation de 2 heures.

Si Amazon EBS n'est pas en mesure de respecter le délai de traitement demandé ou si une demande est annulée en raison de problèmes liés au service, les frais supplémentaires liés à l'opération de copie des instantanés basée sur le temps ne vous sont pas facturés.

Si vous supprimez la copie de l'instantané alors que l'opération de copie de l'instantané basée sur le temps est toujours en cours, les données copiées jusqu'à ce moment vous sont facturées au tarif correspondant à la durée de réalisation spécifiée.

Chiffrement et copie d'instantanés

Note

Le chiffrement côté serveur Amazon S3 (AES 256 bits) protège les données d'un instantané en transit pendant une opération de copie.

Vous pouvez créer une copie instantanée chiffrée d'un instantané source non chiffré. Vous pouvez également chiffrer une copie de l'instantané à l'aide d'une clé KMS différente de l'instantané source. Toutefois, la modification de l'état de chiffrement d'une copie instantanée au cours d'une opération de copie peut entraîner une copie complète (et non incrémentielle), ce qui peut entraîner des frais de transfert et de stockage de données plus élevés.

Tip

Lorsque vous utilisez un instantané chiffré partagé avec vous, nous vous recommandons de le chiffrer à nouveau en le copiant et en utilisant une clé KMS dont vous êtes propriétaire. Cela vous protège si la clé KMS d'origine est compromise ou si le propriétaire révoque votre accès, ce qui pourrait vous faire perdre l'accès au snapshot et à tous les volumes chiffrés que vous avez créés à partir de celui-ci.

Autorisations pour copier des instantanés chiffrés

Pour copier un instantané chiffré, votre utilisateur doit disposer des autorisations suivantes pour utiliser le chiffrement Amazon EBS.

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`
- `kms:Decrypt`
- Pour copier un instantané chiffré qui est partagé depuis un autre AWS compte, vous devez être autorisé à utiliser la clé gérée par le client qui a été utilisée pour chiffrer cet instantané. Pour de plus amples informations, veuillez consulter [Partagez la clé KMS utilisée pour chiffrer un instantané Amazon EBS partagé](#).

Résultats du chiffrement pour les copies instantanées

Le tableau suivant décrit les résultats du chiffrement lorsque vous copiez des instantanés que vous possédez et des instantanés partagés avec vous.

Chiffrement par défaut pour la région de destination	Capture d'écran source	Résultat du chiffrement de la copie instantanée	Remarque
Désactivé	Non chiffré	Chiffrement en option	Si vous chiffrez la copie, vous pouvez spécifier la clé KMS à utiliser. Si vous chiffrez la copie sans spécifier de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.
Désactivé	Encrypted	Chiffré automatiquement	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, le Clé gérée par AWS (aws/ebs) est utilisé.

Chiffrement par défaut pour la région de destination	Capture d'écran source	Résultat du chiffrement de la copie instantanée	Remarque
Activé	Non chiffré	Chiffré automatiquement	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.
Activé	Encrypted	Chiffré automatiquement	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.

Copie d'un instantané

Vous pouvez copier des instantanés d'une région vers une autre. Vous pouvez copier un instantané non chiffré vers un instantané chiffré. Toutefois, si vous tentez de copier un instantané chiffré sans être autorisé à utiliser la clé de chiffrement, l'opération échoue silencieusement et la copie de l'instantané reçoit le message d'état « L'ID de clé donné n'est pas accessible ».

Console

Pour copier un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Sélectionnez l'instantané à copier, puis choisissez Actions, Copy snapshot (Copier l'instantané).
4. Pour Description, saisissez une brève description de la copie de l'instantané.

Par défaut, la description inclut des informations sur l'instantané source afin que vous puissiez distinguer une copie de l'original.

5. Spécifiez la destination de la copie de l'instantané.

- Pour copier l'instantané dans la même région ou dans une autre région, sélectionnez AWS Région, puis sélectionnez la région de destination.
 - Pour copier l'instantané dans une zone locale, sélectionnez Zone AWS locale, puis sélectionnez la zone locale de destination.
 - (Outpostclients uniquement) Pour copier l'instantané vers unOutpost, sélectionnez AWS Outpost puis saisissez l'ARN de la destinationOutpost.
6. Si vous souhaitez que la copie instantanée soit terminée dans un délai précis, sélectionnez Activer la copie basée sur le temps. Pour Durée d'achèvement, entrez la durée d'achèvement requise, par tranches de 15 minutes. Pour plus d'informations, consultez [Time-based copies pour les instantanés et les AMI Amazon EBS EBS-backed](#).

Si vous n'avez pas besoin que la copie instantanée soit terminée dans un délai précis, n'activez pas la copie basée sur le temps. Dans ce cas, la copie instantanée est réalisée dans les meilleurs délais.

7. (Outpostclients uniquement) Pour créer la copie du cliché Outpost dans la région sélectionnée, choisissez Destination du cliché AWS Outpost, puis dans Destination Outpost ARN de destination, entrez l'ARN du Outpost vers lequel vous souhaitez copier le cliché. Le champ Destination de la capture d'écran n'apparaît que si vous avez et Outpost dans la région sélectionnée.
8. Spécifiez l'état du chiffrement pour la copie d'instantané.

Si l'instantané source est chiffré ou si le [chiffrement est activé par défaut sur votre compte](#), la copie de l'instantané est automatiquement chiffrée. Si l'instantané source n'est pas chiffré et que le chiffrement par défaut n'est pas activé pour votre compte, le chiffrement est facultatif.

9. Choisissez Copier un instantané.

AWS CLI

Pour copier un instantané dans une autre région

Utilisez la commande [copy-snapshot](#). L'exemple suivant copie l'instantané spécifié de la région source vers la région actuelle, qui est spécifiée par l'--regionoption.

```
aws ec2 copy-snapshot \  
  --source-snapshot-id snap-0abcdef1234567890 \  
  --source-region us-east-1 \  
  --target-region us-east-1 \  
  --target-snapshot-id target-snapshot-id
```



```
--region us-west-2
```

Pour copier un instantané non chiffré vers un instantané chiffré

Utilisez la commande [copy-snapshot](#). L'exemple suivant copie le cliché non chiffré spécifié de la région source vers la région actuelle, en chiffrant le nouveau cliché à l'aide de la clé KMS spécifiée.

```
aws ec2 copy-snapshot \  
  --source-snapshot-id snap-0abcdef1234567890 \  
  --source-region us-east-1 \  
  --encrypted \  
  --kms-key-id alias/my-kms-key
```

PowerShell

Pour copier un instantané dans une autre région

Utilisez l'applet de commande [Copy-EC2Snapshot](#). L'exemple suivant copie l'instantané spécifié de la région source vers la région actuelle, qui est spécifiée par l'--region option.

```
Copy-EC2Snapshot `   
  -SourceSnapshotId snap-0abcdef1234567890 `   
  -SourceRegion us-east-1 `   
  -Region us-west-2
```

Pour copier un instantané non chiffré vers un instantané chiffré

Utilisez l'applet de commande [Copy-EC2Snapshot](#). L'exemple suivant copie le cliché non chiffré spécifié de la région source vers la région actuelle, en chiffrant le nouveau cliché à l'aide de la clé KMS spécifiée.

```
Copy-EC2Snapshot `   
  -SourceSnapshotId snap-0abcdef1234567890 `   
  -SourceRegion us-east-1 `   
  -Encrypted $true `   
  -KmsKeyId alias/my-kms-key
```

Partager un instantané Amazon EBS avec d'autres AWS comptes

Vous pouvez modifier les autorisations d'un instantané si vous souhaitez partager celui-ci avec d'autres comptes AWS . Vous pouvez partager des instantanés publiquement avec tous les autres AWS comptes, ou vous pouvez les partager en privé avec les AWS comptes individuels que vous spécifiez. Les utilisateurs qui bénéficient de votre autorisation peuvent utiliser les instantanés que vous partagez pour créer leurs propres volumes EBS, tandis que votre instantané d'origine reste inchangé.

Important

Lorsque vous partagez un instantané, vous autorisez d'autres personnes à accéder à toutes les données de l'instantané. Partagez vos instantanés uniquement avec les personnes à qui vous faites confiance pour toutes vos données d'instantané.

Pour empêcher le partage public des instantanés, vous pouvez activer [Bloquer l'accès public aux instantanés Amazon EBS](#).

Rubriques

- [Avant de partager un instantané](#)
- [Partager un instantané](#)
- [Partagez la clé KMS utilisée pour chiffrer un instantané Amazon EBS partagé](#)
- [Utilisez les instantanés Amazon EBS qui sont partagés avec vous](#)
- [Déterminer l'utilisation des instantanés que vous partagez](#)

Avant de partager un instantané

Les considérations suivantes s'appliquent au partage des instantanés :

- Si le blocage de l'accès public pour les instantanés est activé pour la région, les tentatives de partage public des instantanés seront bloquées. Les instantanés peuvent toujours être partagés en privé.
- Les instantanés sont limités à la région dans laquelle ils ont été créés. Pour partager un instantané avec une autre région, copiez l'instantané dans cette région, puis partagez la copie. Pour de plus amples informations, veuillez consulter [Copier un instantané Amazon EBS](#).

- Vous ne pouvez pas partager d'instantanés chiffrés avec l' Clé gérée par AWS par défaut. Vous ne pouvez pas partager d'instantanés chiffrés avec une clé gérée par le client. Pour plus d'informations, consultez [Création des clés](#) dans le Guide du développeur AWS Key Management Service .
- Vous ne pouvez partager que des instantanés non chiffrés publiquement.
- Lorsque vous partagez un instantané chiffré, vous devez également partager la clé gérée par le client qui a servi à chiffrer l'instantané. Pour plus d'informations, consultez [Partagez la clé KMS utilisée pour chiffrer un instantané Amazon EBS partagé](#).

Partager un instantané

Vous pouvez partager un instantané publiquement ou avec des AWS comptes spécifiques.

Console

Pour partager un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Sélectionnez l'instantané à partager, puis choisissez Actions, Modify permissions (Modifier des autorisations).
4. Spécifiez les autorisations de l'instantané. Current setting (Paramétrage actuel) indique les autorisations de partage actuelles de l'instantané.
 - Pour partager l'instantané publiquement avec tous les AWS comptes, choisissez Public.
 - Pour partager l'instantané en privé avec des AWS comptes spécifiques, choisissez Privé. Ensuite, dans la section Sharing accounts (Partage de comptes), choisissez Add account (Ajouter un compte), puis saisissez l'ID de compte à 12 chiffres (sans traits d'union) du compte avec lequel partager.
5. Sélectionnez Enregistrer les modifications.

AWS CLI

Les autorisations pour un instantané sont spécifiées à l'aide de l'attribut `createVolumePermission` de l'instantané. Pour qu'un instantané devienne public, définissez le groupe sur `all`. Pour partager un instantané avec un AWS compte spécifique, définissez l'ID du AWS compte pour l'utilisateur.

Pour partager un instantané en mode public

Utilisez la commande [modify-snapshot-attribute](#).

Pour `--attribute`, spécifiez `createVolumePermission`. Pour `--operation-type`, spécifiez `add`. Pour `--group-names`, spécifiez `all`.

```
aws ec2 modify-snapshot-attribute \  
  --snapshot-id snap-0abcdef1234567890 \  
  --attribute createVolumePermission \  
  --operation-type add \  
  --group-names all
```

Pour partager un instantané en mode privé

Utilisez la commande [modify-snapshot-attribute](#).

Pour `--attribute`, spécifiez `createVolumePermission`. Pour `--operation-type`, spécifiez `add`. Pour `--user-ids`, spécifiez les identifiants à 12 chiffres des AWS comptes avec lesquels vous souhaitez partager les instantanés.

```
aws ec2 modify-snapshot-attribute \  
  --snapshot-id snap-0abcdef1234567890 \  
  --attribute createVolumePermission \  
  --operation-type add \  
  --user-ids 123456789012 111122223333
```

PowerShell

Les autorisations pour un instantané sont spécifiées à l'aide de l'attribut `createVolumePermission` de l'instantané. Pour qu'un instantané devienne public, définissez le groupe sur `all`. Pour partager un instantané avec un AWS compte spécifique, définissez l'ID du AWS compte pour l'utilisateur.

Pour partager un instantané en mode public

Utilisez l'applet de commande [Edit-EC2SnapshotAttribute](#).

Pour `-Attribute`, spécifiez `CreateVolumePermission`. Pour `-OperationType`, spécifiez `Add`. Pour `-GroupName`, spécifiez `all`.

```
Edit-EC2SnapshotAttribute `\  
  -SnapshotId snap-0abcdef1234567890 `
```

```
-Attribute CreateVolumePermission `
-OperationType Add `
-GroupName all
```

Pour partager un instantané en mode privé

Utilisez l'applet de commande [Edit-EC2SnapshotAttribute](#).

Pour `-Attribute`, spécifiez `CreateVolumePermission`. Pour `-OperationType`, spécifiez `Add`. Pour `UserId`, spécifiez les identifiants à 12 chiffres des AWS comptes avec lesquels vous souhaitez partager les instantanés.

```
Edit-EC2SnapshotAttribute `
-SnapshotId snap-0abcdef1234567890 `
-Attribute CreateVolumePermission `
-OperationType Add `
-UserId 123456789012 111122223333
```

Partagez la clé KMS utilisée pour chiffrer un instantané Amazon EBS partagé

Lorsque vous partagez un instantané chiffré, vous devez également partager la clé gérée par le client qui a servi à chiffrer l'instantané. Vous pouvez appliquer des autorisations inter-comptes à une clé gérée par le client lors de sa création ou ultérieurement.

Les utilisateurs de votre clé gérée par le client partagée qui accèdent aux instantanés chiffrés doivent recevoir les autorisations permettant d'exécuter les actions suivantes sur la clé :

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`
- `kms:Decrypt`

Tip

Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition

pour permettre à l'utilisateur de créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée pour le compte de l'utilisateur par un AWS service.

Pour en savoir plus sur le contrôle de l'accès à une clé gérée par le client, consultez [Utilisation de stratégies de clé dans AWS KMS](#) dans le Guide du développeur AWS Key Management Service .

Pour partager la clé gérée par le client à l'aide du AWS KMS console

1. Ouvrez la AWS KMS console à l'adresse <https://console.aws.amazon.com/kms>.
2. Pour modifier la Région AWS, utilisez le sélecteur de région situé dans le coin supérieur droit de la page.
3. Choisissez Customer managed keys (Clés gérées par le client) dans le volet de navigation.
4. Dans la colonne Alias choisissez l'alias (lien texte) de la clé gérée par le client que vous avez utilisée pour chiffrer l'instantané. Les détails de la clé s'ouvrent dans une nouvelle page.
5. Dans la section Key policy (Stratégie de clé) s'affiche soit la vue de la stratégie soit la vue par défaut. La vue de la politique affiche le document de la politique de clé. La vue par défaut affiche les sections Key administrators (Administrateurs de clé), Key deletion (Suppression de clé), Key Use (Utilisation de clé) et Other AWS accounts (Autres comptes). L'affichage par défaut s'affiche si vous avez créé la politique dans la console et que vous ne l'avez pas personnalisée. Si l'affichage par défaut n'est pas disponible, vous devez modifier manuellement la politique dans l'affichage de politique. Pour plus d'informations, consultez [Affichage d'une stratégie de clé \(console\)](#) dans le Guide du développeur AWS Key Management Service .

Utilisez la vue des règles ou la vue par défaut, selon la vue à laquelle vous pouvez accéder, pour ajouter un ou plusieurs identifiants de AWS compte à la politique, comme suit :

- (Vue de la stratégie) Choisissez Edit (Modifier). Ajoutez un ou plusieurs identifiants de AWS compte aux relevés suivants : "Allow use of the key" et "Allow attachment of persistent resources". Sélectionnez Enregistrer les modifications. Dans l'exemple suivant, l'ID de AWS compte 444455556666 est ajouté à la politique.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
```

```

    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  },
  {
    "Sid": "Allow attachment of persistent resources",
    "Effect": "Allow",
    "Principal": {"AWS": [
      "arn:aws:iam::111122223333:user/KeyUser",
      "arn:aws:iam::444455556666:root"
    ]},
    "Action": [
      "kms:CreateGrant",
      "kms:ListGrants",
      "kms:RevokeGrant"
    ],
    "Resource": "*",
    "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
  }
}

```

- (Affichage par défaut) Faites défiler la page jusqu'à Autres AWS comptes. Choisissez Ajouter d'autres AWS comptes et saisissez l'identifiant du AWS compte comme demandé. Pour ajouter un autre compte, choisissez Ajouter un autre AWS compte et saisissez l'identifiant du AWS compte. Une fois que vous avez ajouté tous les comptes AWS , choisissez Enregistrer les modifications.

Utilisez les instantanés Amazon EBS qui sont partagés avec vous

Pour utiliser un instantané partagé non chiffré

Localisez l'instantané partagé par son ID ou sa description. Vous pouvez utiliser cet instantané comme n'importe quel autre instantané que vous possédez dans votre compte. Par exemple, vous pouvez créer un volume à partir de l'instantané ou le copier dans une autre région.

Pour utiliser un instantané chiffré partagé

Localisez l'instantané partagé par son ID ou sa description. Créez une copie de l'instantané partagé dans votre compte et chiffrez la copie à l'aide d'une clé KMS que vous possédez. Vous pouvez ensuite utiliser la copie pour créer des volumes ou la copier dans différentes régions.

Console

Pour afficher les autorisations relatives aux instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané.
4. Si le filtre m'appartient, l'instantané appartient à ce compte. Si le filtre est Instantanés privés, l'instantané appartient à ce compte ou est partagé spécifiquement avec ce compte. Sélectionnez un instantané et, dans l'onglet Détails, vérifiez si le propriétaire spécifie ce compte ou un autre compte.

AWS CLI

Pour afficher les autorisations relatives aux instantanés

Utilisez la [commande](#) `describe-snapshot-attribute` pour obtenir les autorisations de capture instantanée du cliché spécifié.

```
aws ec2 describe-snapshot-attribute \  
  --snapshot-id snap-0abcdef1234567890 \  
  --attribute createVolumePermission
```

Voici un exemple de sortie.

```
{  
  "SnapshotId": "snap-0abcdef1234567890",  
  "CreateVolumePermissions": [  
    {  
      "UserId": "111122223333"  
    }  
  ]  
}
```


PowerShell

Pour afficher les autorisations relatives aux instantanés

Utilisez l'applet de commande [Get-EC2SnapshotAttribute](#).

```
(Get-EC2SnapshotAttribute `
  -SnapshotId snap-0abcdef1234567890 `
  -Attribute createVolumePermission).CreateVolumePermissions
```

Voici un exemple de sortie.

```
Group UserId
-----
111122223333
```

Déterminer l'utilisation des instantanés que vous partagez

Vous pouvez l'utiliser AWS CloudTrail pour contrôler si un instantané que vous avez partagé avec d'autres personnes est copié ou utilisé pour créer un volume. Les événements suivants sont enregistrés CloudTrail lorsqu'une action est effectuée sur un instantané que vous avez partagé :

- SharedSnapshotCopyInitiated— Un instantané partagé est en cours de copie.
- SharedSnapshotVolumeCreated— Un instantané partagé est utilisé pour créer un volume.

Pour plus d'informations sur l'utilisation CloudTrail, consultez [Consigner les appels d'API Amazon EC2 et Amazon EBS avec AWS CloudTrail](#)

Archiver des instantanés Amazon EBS

L'archive d'instantanés Amazon EBS est un niveau de stockage que vous pouvez utiliser pour le stockage à long terme et à faible coût de vos instantanés rarement consultés qui ne nécessitent pas d'extraction fréquente ou rapide.

Par défaut, lorsque vous créez un instantané, il est stocké dans le niveau Amazon EBS Snapshot Standard (niveau standard). Les instantanés stockés dans le niveau standard sont incrémentiels. Cela signifie que seuls les blocs du volume qui ont été modifiés après votre dernier instantané sont sauvegardés.

Lorsque vous archivez un instantané, l'instantané incrémentiel est converti en instantané complet et il est déplacé du niveau standard vers le niveau Amazon EBS Snapshots Archive (niveau d'archivage). Les instantanés complets incluent tous les blocs écrits sur le volume au moment de la création de l'instantané.

Lorsque vous devez accéder à un instantané archivé, vous pouvez le restaurer depuis le niveau d'archivage vers le niveau standard, puis l'utiliser de la même manière que n'importe quel autre instantané de votre compte.

Amazon EBS Snapshots Archive offre des coûts de stockage d'instantanés jusqu'à 75 % inférieurs pour les instantanés que vous prévoyez de stocker pendant 90 jours ou plus et auxquels vous n'avez que rarement besoin d'accéder.

Les cas d'utilisation typiques incluent :

- l'archivage du seul instantané d'un volume, comme les instantanés de fin de projet ;
- l'archivage des instantanés incrémentiels complets et ponctuels pour des raisons de conformité ;
- l'archivage des instantanés incrémentiels mensuels, trimestriels ou annuels.

Rubriques

- [Quotas](#)
- [Considérations et limites relatives à l'archivage des instantanés Amazon EBS](#)
- [Tarification et facturation pour l'archivage des instantanés Amazon EBS](#)
- [Directives et bonnes pratiques pour l'archivage des instantanés Amazon EBS](#)
- [Autorisations IAM requises pour l'archivage des instantanés Amazon EBS](#)
- [Archiver un instantané Amazon EBS](#)
- [Restaurer un instantané Amazon EBS archivé](#)
- [Modifier la période de restauration pour un instantané Amazon EBS temporairement restauré](#)
- [Afficher les instantanés Amazon EBS archivés](#)
- [Surveillez l'archivage des instantanés Amazon EBS à l'aide d'événements CloudWatch](#)

Quotas

Cette section décrit les quotas par défaut pour les instantanés archivés et en cours de réalisation.

Quota	Quota par défaut			
Instantanés archivés par volume	25			
Archives simultanées d'instantanés en cours par compte	25			
Restaurations simultanées d'instantanés en cours par compte	5			

Si vous avez besoin de plus que les limites par défaut, complétez le [formulaire Support Center](#) Create case pour demander une augmentation de la limite.

Considérations et limites relatives à l'archivage des instantanés Amazon EBS

Gardez les points suivants à l'esprit lorsque vous archivez des instantanés Amazon EBS.

Considérations

- La période d'archivage minimale est de 90 jours. Si vous supprimez ou restaurez définitivement un instantané archivé avant la période d'archivage minimale de 90 jours, vous êtes facturé pour les

jours restants dans le niveau d'archivage, arrondi à l'heure la plus proche. Pour plus d'informations, consultez [Tarification et facturation pour l'archivage des instantanés Amazon EBS](#).

- La restauration d'un instantané archivé du niveau d'archivage au niveau standard peut prendre jusqu'à 72 heures, en fonction de la taille de l'instantané.
- Les instantanés archivés sont toujours des instantanés complets. Les instantanés complets incluent tous les blocs écrits sur le volume au moment de la création de l'instantané. L'instantané complet sera probablement plus grand que l'instantané incrémentiel à partir duquel il a été créé. Toutefois, si vous ne disposez que d'un seul instantané d'un volume au niveau standard, la taille de l'instantané complet au niveau d'archivage sera la même que celle de l'instantané au niveau standard. En effet, le premier instantané pris d'un volume est toujours un instantané complet. Pour obtenir la taille complète de l'instantané, utilisez la commande [describe-snapshots](#) AWS CLI .
- L'archivage est recommandé pour les instantanés mensuels, trimestriels ou annuels. L'archivage quotidien d'instantanés incrémentiels d'un seul volume peut entraîner des coûts plus élevés par rapport à leur conservation dans le niveau standard.
- Lorsqu'un instantané est archivé, ses données référencées par d'autres instantanés dans sa lignée sont retenues dans le niveau standard. Les coûts de données et de stockage associés aux données référencées retenues sur le niveau standard sont alloués au prochain instantané de la lignée. Cela garantit que les instantanés suivants dans la lignée ne sont pas affectés par l'archivage.
- Si vous supprimez un instantané archivé qui correspond à une règle de rétention de la corbeille, l'instantané archivé est retenu dans la corbeille pendant la période définie dans la règle de rétention. Pour utiliser cet instantané, vous devez d'abord le récupérer depuis la corbeille, puis le restaurer à partir du niveau d'archivage. Pour plus d'informations, voir [Corbeille](#) et [Tarification et facturation pour l'archivage des instantanés Amazon EBS](#).
- Vous ne pouvez pas utiliser un instantané archivé dans un mappage de périphérique de stockage en mode bloc ou pour créer un volume Amazon EBS.
- Vous pouvez archiver les instantanés créés AWS Backup à l'aide des Console AWS Backup API ou des outils de ligne de commande. Pour de plus amples informations, consultez [Création d'un plan de sauvegarde](#) dans le Guide du développeur AWS Backup .

Limitations

- Vous ne pouvez archiver que les instantanés dont l'état est `completed`.

- Vous ne pouvez archiver que les instantanés dont vous êtes propriétaire dans votre compte. Pour archiver un instantané qui vous est partagé, copiez d'abord l'instantané sur votre compte, puis archivez la copie de l'instantané.
- Avant de pouvoir utiliser un instantané archivé, vous devez d'abord le restaurer au niveau standard. La restauration vers le niveau standard est nécessaire pour créer un volume à partir de l'instantané via les opérations d'API `CreateVolume` et `RunInstances`, ainsi que pour partager ou copier un instantané. Pour de plus amples informations, veuillez consulter [Restaurer un instantané Amazon EBS archivé](#).
- Vous ne pouvez archiver un instantané associé à une ou plusieurs AMI que si toutes les AMI associées sont désactivées. Pour plus d'informations, voir [Désactiver une AMI](#).
- Vous ne pouvez pas activer une AMI désactivée si les instantanés associés sont temporairement restaurés. Tous les instantanés associés doivent être définitivement restaurés avant que vous puissiez activer l'AMI.
- Vous ne pouvez pas annuler le processus d'archivage des instantanés ou de restauration des instantanés une fois qu'il a été démarré.
- Vous ne pouvez pas partager les instantanés archivés. Si vous archivez un instantané que vous avez partagé avec d'autres comptes, les comptes avec lesquels l'instantané est partagé perdent l'accès une fois l'instantané archivé.
- Vous ne pouvez pas copier les instantanés archivés. Si vous devez copier un instantané archivé, vous devez d'abord le restaurer.
- Vous ne pouvez pas activer la restauration rapide d'instantané pour un instantané archivé. La restauration rapide d'instantané est automatiquement désactivée lorsqu'un instantané est archivé. Si vous devez utiliser la restauration d'instantané rapide, vous devez l'activer manuellement après la restauration de l'instantané.

Tarification et facturation pour l'archivage des instantanés Amazon EBS

Les instantanés archivés sont facturés au tarif de 0,0125\$ par. GB-month Par exemple, si vous archivez un instantané de 100 Gio, vous êtes facturé 1,25 USD (100 Gio * 0,0125 USD/Gio) par mois.

Les restaurations d'instantanés sont facturées au tarif de 0,03 USD par Go de données restaurées. Par exemple, si vous restaurez un instantané de 100 Gio à partir du niveau d'archivage, vous êtes facturé une fois 3 USD (100 Gio * 0,03 USD/Gio).

Une fois que l'instantané est restauré au niveau standard, il est facturé au tarif standard pour les instantanés de 0,05 USD par. GB-month

Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Facturation pour la période d'archivage minimale

La période d'archivage minimale est de 90 jours. Si vous supprimez ou restaurez définitivement un instantané archivé avant la période d'archivage minimale de 90 jours, vous êtes facturé au prorata des frais de stockage du niveau d'archivage pour les jours restants, arrondis à l'heure la plus proche. Par exemple, si vous supprimez ou restaurez définitivement un instantané archivé après 40 jours, vous êtes facturé pour les 50 jours restants de la période d'archivage minimale.

Note

La restauration temporaire d'un instantané archivé avant la période d'archivage minimale de 90 jours n'entraîne pas ces frais.

Restauration temporaire

Lorsque vous restaurez temporairement un instantané, l'instantané est restauré du niveau d'archivage vers le niveau standard, et une copie de l'instantané reste dans le niveau d'archivage. Vous êtes facturé à la fois pour l'instantané dans le niveau standard et pour la copie d'instantané dans le niveau d'archivage pendant la durée de la période de restauration temporaire. Lorsque l'instantané temporairement restauré est retiré du niveau standard, vous n'êtes plus facturé pour celui-ci (niveau standard), et vous êtes facturé pour l'instantané dans le niveau d'archivage uniquement.

Restauration définitive

Lorsque vous restaurez définitivement un instantané, l'instantané est restauré du niveau d'archivage vers le niveau standard, et l'instantané est supprimé du niveau d'archivage. Vous êtes facturé pour l'instantané uniquement dans le niveau standard.

Suppression d'instantanés

Si vous supprimez un instantané pendant qu'il est archivé, vous êtes facturé pour les données de l'instantané qui ont déjà été déplacées vers le niveau d'archivage. Ces données sont soumises à la période d'archivage minimale de 90 jours et facturées en conséquence lors de leur suppression. Par exemple, si vous archivez un instantané de 100 Go et que vous le supprimez après seulement 40 Go

d'archivage, vous êtes facturé 1,50\$ pour la période d'archivage minimale de 90 jours pour les 40 Go déjà archivés ($0,0125 \text{ USD par GB-month} * 40 \text{ Go} * (90 \text{ jours} * 24 \text{ heures}) / (24 * 30 \text{ jours par mois})$).
hours/day

Si vous supprimez un instantané alors qu'il est restauré à partir du niveau d'archivage, la restauration de l'instantané vous sera facturée pour sa taille réelle (taille de l'instantané * 0,03 USD). Par exemple, si vous restaurez un instantané de 100 Gio à partir du niveau d'archivage et que vous supprimez l'instantané à n'importe quel moment avant la fin de sa restauration, vous êtes facturé 3 USD (taille d'instantané de 100 Gio * 0,03 USD).

Corbeille

Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille. Les instantanés archivés qui se trouvent dans la corbeille sont soumis à la période d'archivage minimale de 90 jours et sont facturés en conséquence s'ils sont supprimés par la corbeille avant la période d'archivage minimale. En d'autres termes, si une règle de rétention supprime un instantané archivé de la corbeille avant la période minimale de 90 jours, vous êtes facturé pour les jours restants.

Si vous supprimez un instantané correspondant à une règle de rétention pendant l'archivage de l'instantané, l'instantané archivé est retenu dans la corbeille pendant la période de rétention définie dans la règle de rétention. Il est facturé au tarif des instantanés archivés.

Si vous supprimez un instantané correspondant à une règle de rétention pendant la restauration de l'instantané, l'instantané restauré est retenu dans la corbeille pendant le reste de la période de rétention, et facturé au taux d'instantané standard. Pour utiliser l'instantané restauré, vous devez d'abord le récupérer depuis la corbeille.

Pour plus d'informations, voir [Corbeille](#).

Suivi des coûts

Les instantanés archivés apparaissent dans le AWS Cost and Usage Report avec le même ID de ressource et le même Amazon Resource Name (ARN). Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Cost and Usage Report](#).

Vous pouvez utiliser les types d'utilisation suivants pour identifier les coûts associés :

- SnapshotArchiveStorage : frais pour le stockage de données mensuel
- SnapshotArchiveRetrieval : frais ponctuels pour les restaurations d'instantanés

- `SnapshotArchiveEarlyDelete` : frais de suppression ou de restauration permanente d'un instantané avant la période d'archivage minimale (90 jours)

Directives et bonnes pratiques pour l'archivage des instantanés Amazon EBS

Cette section fournit des consignes et de bonnes pratiques pour l'archivage des instantanés.

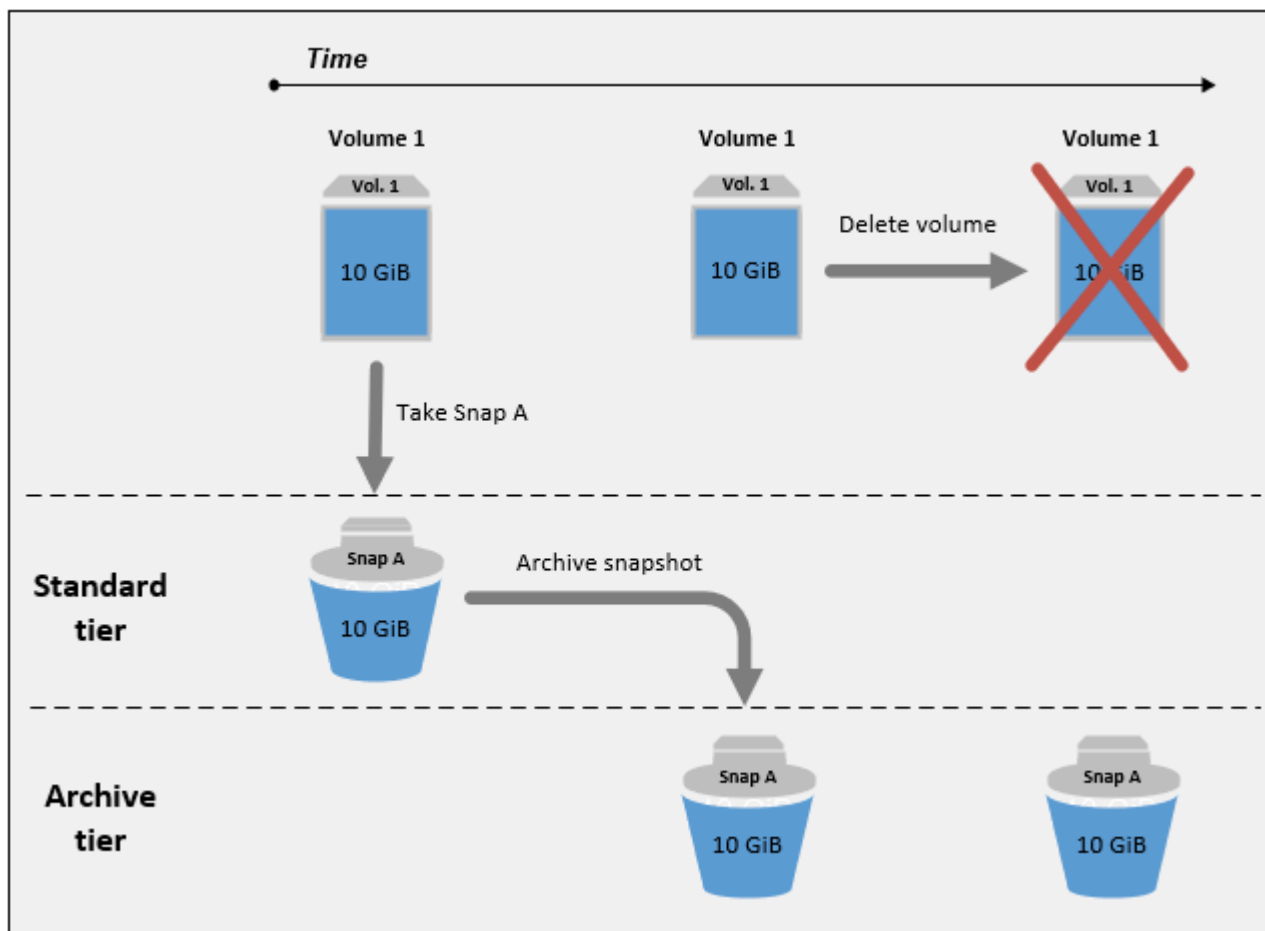
Rubriques

- [Archivage du seul instantané d'un volume](#)
- [Archivage des instantanés incrémentiels d'un seul volume](#)
- [Archivage des instantanés complets pour des raisons de conformité](#)
- [Évaluation de la réduction des coûts de stockage de niveau standard](#)

Archivage du seul instantané d'un volume

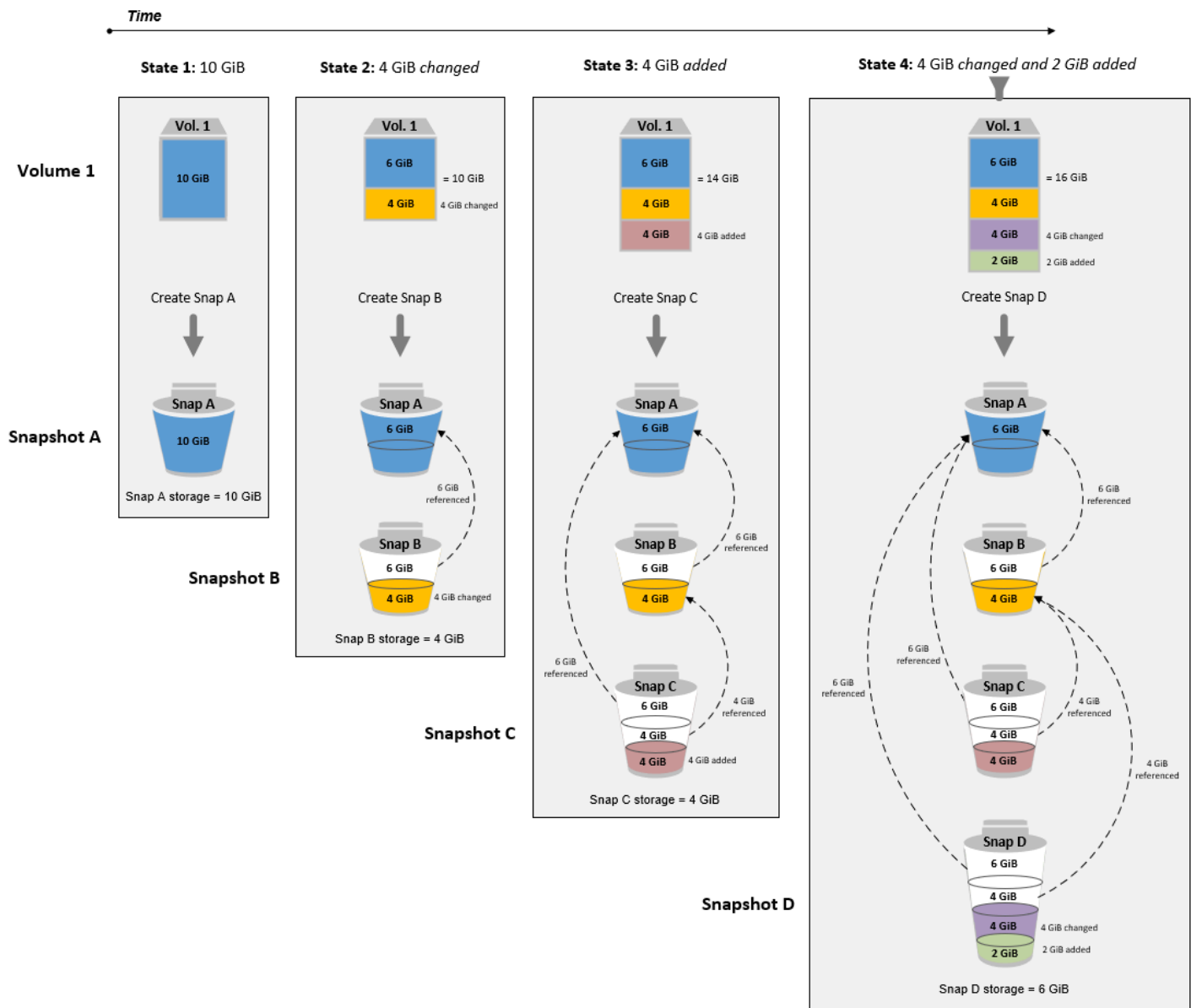
Lorsque vous n'avez qu'un seul instantané d'un volume, l'instantané a toujours la même taille que les blocs écrits sur le volume au moment de la création de l'instantané. Lorsque vous archivez un tel instantané, l'instantané du niveau standard est converti en instantané complet de taille équivalente et il est déplacé du niveau standard vers le niveau d'archivage.

L'archivage de ces instantanés peut vous aider à économiser avec des coûts de stockage réduits. Si vous n'avez plus besoin du volume source, vous pouvez le supprimer pour réduire davantage les coûts de stockage.



Archivage des instantanés incrémentiels d'un seul volume

Lorsque vous archivez un instantané incrémentiel, l'instantané est converti en instantané complet et il est déplacé vers le niveau d'archivage. Par exemple, dans l'image suivante, si vous archivez Snap B, l'instantané est converti en un instantané complet d'une taille de 10 Gio et déplacé vers le niveau d'archivage. De même, si vous archivez Snap C, la taille de l'instantané complet dans le niveau d'archivage est de 14 Gio.



Si vous archivez des instantanés pour réduire vos coûts de stockage dans le niveau standard, n'archivez pas le premier instantané d'un ensemble d'instancés incrémentiels. Ces instantanés sont référencés par les instantanés suivants dans la lignée des instantanés. Dans la plupart des cas, l'archivage de ces instantanés ne réduira pas les coûts de stockage.

Note

N'archivez pas le dernier instantané d'un ensemble d'instancés incrémentiels. Le dernier instantané est l'instantané le plus récent d'un volume. Vous aurez besoin de cet instantané

dans le niveau standard si vous souhaitez créer des volumes à partir de celui-ci en cas de corruption ou de perte de volume.

Si vous archivez un instantané qui contient des données référencées par un instantané ultérieur de la lignée, le stockage des données et les coûts de stockage associés aux données référencées sont attribués à l'instantané ultérieur de la lignée. Dans ce cas, l'archivage de l'instantané ne réduira pas le stockage de données ni les coûts de stockage. Par exemple, dans l'image précédente, si vous archivez Snap B, ses 4 Gio de données sont attribués à Snap C. Dans ce cas, vos coûts de stockage globaux augmenteront, car vous engagez des coûts de stockage pour la version complète de Snap B dans le niveau d'archivage, et vos coûts de stockage pour le niveau standard restent inchangés.

Si vous archivez Snap C, votre stockage de niveau standard diminuera de 4 Gio, car les données ne sont référencées par aucun autre instantané ultérieur dans la lignée. De plus, votre stockage de niveau d'archivage augmentera de 14 Gio, car l'instantané est converti en instantané complet.

Archivage des instantanés complets pour des raisons de conformité

Vous devrez peut-être créer des sauvegardes complètes de volumes sur une base mensuelle, trimestrielle ou annuelle pour des raisons de conformité. Pour ces sauvegardes, vous pouvez avoir besoin d'instantanés autonomes sans références en amont ou en aval à d'autres instantanés dans la lignée des instantanés. Les instantanés archivés avec EBS Snapshots Archive sont des instantanés complets, et ils ne contiennent aucune référence à d'autres instantanés de la lignée. En outre, vous devrez probablement retenir ces instantanés pour des raisons de conformité pendant plusieurs années. EBS Snapshots Archive permet d'archiver de manière rentable ces instantanés complets pour une rétention à long terme.

Évaluation de la réduction des coûts de stockage de niveau standard

Si vous souhaitez archiver un instantané incrémentiel pour réduire vos coûts de stockage, vous devez prendre en compte la taille de l'instantané complet dans le niveau d'archivage et la réduction du stockage dans le niveau standard. Cette section explique comment procéder.

Important

Les réponses de l'API sont des données précises au moment où les API sont appelées. Les réponses de l'API peuvent différer lorsque les données associées à un instantané changent suite à des modifications de la lignée de ce dernier.

Pour déterminer la réduction du stockage et des coûts de stockage dans le niveau standard, procédez comme suit.

1. Pour le cliché que vous souhaitez archiver, vérifiez sa taille complète et le volume source à partir duquel il a été créé. Utilisez la [commande](#) `describe-snapshots` et, pour `--snapshot-id`, spécifiez l'ID du cliché que vous souhaitez archiver.

```
$ aws ec2 describe-snapshots --snapshot-id snapshot_id
```

La `FullSnapshotSizeInBytes` valeur de réponse indique la taille complète de l'instantané, en octets, et la valeur de `VolumeId` réponse indique l'ID du volume source.

Par exemple, la commande suivante renvoie des informations sur l'instantané `snap-09c9114207084f0d9`.

```
$ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
```

L'exemple de sortie suivant montre que la taille complète de l'instantané est d'`5678912341` octets (5,28 GiB) et que le volume source est de `vol-0f3e2c292c52b85c3`

```
{
  "Snapshots": [
    {
      "Description": "",
      "Tags": [],
      "Encrypted": false,
      "VolumeId": "vol-0f3e2c292c52b85c3",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2021-11-16T08:29:49.840Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "FullSnapshotSizeInBytes" : "5678912341",
      "SnapshotId": "snap-09c9114207084f0d9"
    }
  ]
}
```

2. Cherchez tous les instantanés créés à partir du volume source. Utilisez la commande [describe-snapshots](#). Spécifiez le filtre `volume-id`, et pour la valeur du filtre, spécifiez l'ID du volume de l'étape précédente.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

Par exemple, la commande suivante renvoie tous les instantanés créés à partir du volume `vol-0f3e2c292c52b85c3`.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id,  
Values=vol-0f3e2c292c52b85c3"
```

Voici la sortie de la commande, qui indique que trois instantanés ont été créés à partir du volume `vol-0f3e2c292c52b85c3`.

```
{  
  "Snapshots": [  
    {  
      "Description": "",  
      "Tags": [],  
      "Encrypted": false,  
      "VolumeId": "vol-0f3e2c292c52b85c3",  
      "State": "completed",  
      "VolumeSize": 8,  
      "StartTime": "2021-11-14T08:57:39.300Z",  
      "Progress": "100%",  
      "OwnerId": "123456789012",  
      "SnapshotId": "snap-08ca60083f86816b0"  
    },  
    {  
      "Description": "",  
      "Tags": [],  
      "Encrypted": false,  
      "VolumeId": "vol-0f3e2c292c52b85c3",  
      "State": "completed",  
      "VolumeSize": 8,  
      "StartTime": "2021-11-15T08:29:49.840Z",  
      "Progress": "100%",  
      "OwnerId": "123456789012",  
      "SnapshotId": "snap-09c9114207084f0d9"  
    },  
    {  
      "Description": "",  
      "Tags": [],  
      "Encrypted": false,  
      "VolumeId": "vol-0f3e2c292c52b85c3",  
      "State": "completed",  
      "VolumeSize": 8,  
      "StartTime": "2021-11-16T08:12:34.560Z",  
      "Progress": "100%",  
      "OwnerId": "123456789012",  
      "SnapshotId": "snap-0a1b2c3d4e5f67890"  
    }  
  ]  
}
```

```
{
  "Description": "01",
  "Tags": [],
  "Encrypted": false,
  "VolumeId": "vol-0f3e2c292c52b85c3",
  "State": "completed",
  "VolumeSize": 8,
  "StartTime": "2021-11-16T07:50:08.042Z",
  "Progress": "100%",
  "OwnerId": "123456789012",
  "SnapshotId": "snap-024f49fe8dd853fa8"
}
```

3. À l'aide du résultat de la commande précédente, trie les instantanés en fonction de leur date de création, du plus ancien au plus récent. Le paramètre de réponse `StartTime` pour chaque instantané indique sa date de création, au format UTC.

Par exemple, les instantanés renvoyés à l'étape précédente, classés par date de création, du plus ancien au plus récent, sont les suivants :

1. `snap-08ca60083f86816b0` (le plus ancien : créé avant l'instantané que vous souhaitez archiver)
2. `snap-09c9114207084f0d9` (l'instantané à archiver)
3. `snap-024f49fe8dd853fa8` (le plus récent, créé après l'instantané que vous souhaitez archiver)
4. Identifiez les instantanés créés immédiatement avant et après l'instantané que vous souhaitez archiver. Dans ce cas, vous souhaitez archiver l'instantané `snap-09c9114207084f0d9`, qui était le deuxième instantané incrémentiel créé dans l'ensemble de trois instantanés. L'instantané `snap-08ca60083f86816b0` a été créé immédiatement avant, et l'instantané `snap-024f49fe8dd853fa8` a été créé immédiatement après.
5. Cherchez les données non référencées dans l'instantané que vous voulez archiver. Tout d'abord, recherchez les blocs qui diffèrent entre l'instantané créé immédiatement avant l'instantané que vous souhaitez archiver et l'instantané que vous souhaitez archiver. Utilisez la commande [list-changed-blocks](#). Pour `--first-snapshot-id`, spécifiez l'ID de l'instantané créé immédiatement avant celui que vous souhaitez archiver. Pour `--second-snapshot-id`, spécifiez l'ID de l'instantané que vous souhaitez archiver.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-snapshot-id snapshot_to_archive
```

Par exemple, la commande suivante affiche les index de blocs pour les blocs qui sont différents entre l'instantané snap-08ca60083f86816b0 (créé avant celui que vous souhaitez archiver) et l'instantané snap-09c9114207084f0d9 (celui que vous souhaitez archiver).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-snapshot-id snap-09c9114207084f0d9
```

Voici la sortie de la commande, certains blocs étant omis.

```
{
  "BlockSize": 524288,
  "ChangedBlocks": [
    {
      "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1r0VeFbWXsH3W4z/",
      "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
      "BlockIndex": 4
    },
    {
      "FirstBlockToken": "ABgBACfL
+EfmQm1NgstqrFnYgsAxR4SDS04LkNLY00ChGBWcfJnnpn90E9XX1",
      "SecondBlockToken": "ABgBAdX0mtX6aBAAt3EBy
+8jFCESMpig7csKjb020cd08m2iNJV2Ue+cRwUqF",
      "BlockIndex": 5
    },
    {
      "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUI3MKZmEMxs2wC3AmM/
fc6yCOAmb65",
      "SecondBlockToken":
"ABgBADewWkHKTCrhZmsfM7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
      "BlockIndex": 13
    },
    {
      "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVn0qPxmx9r7Wf60+i
+ltZ0dwPpGN39ijztLn",
      "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRc1nV
+bKjViu/9UESTcW7CD9w4J2td",
```

```

        "BlockIndex": 14
    },
    {
        "FirstBlockToken":
"ABgBAZBfEv4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICG1FmZCyJXzE4r3",
        "SecondBlockToken":
"ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVCldnpc91zBiNmSfW9ouIlbeXWy",
        "BlockIndex": 15
    },
    ....
    {
        "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5V05Q3rEEA
+ku50P498hjnTAgMhLG",
        "BlockIndex": 13171
    },
    {
        "SecondBlockToken":
"ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
        "BlockIndex": 13172
    },
    {
        "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWi0uj0AKcau0nUFC0
+eZ5ASVdWLXWwC04ijfoDTpTVZ",
        "BlockIndex": 13173
    },
    {
        "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6t0vMoLBLJ14LKvavw4IiB1d0iykWe6b",
        "BlockIndex": 13174
    },
    {
        "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
        "BlockIndex": 13175
    }
],
"ExpiryTime": 1637648751.813,
"VolumeSize": 8
}

```

Ensuite, utilisez la même commande pour rechercher des blocs différents entre l'instantané que vous souhaitez archiver et l'instantané créé immédiatement après. Pour `--first-snapshot-`

id, spécifiez l'ID de l'instantané que vous souhaitez archiver. Pour `--second-snapshot-id`, indiquez l'ID de l'instantané créé immédiatement après l'instantané que vous souhaitez archiver.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-snapshot-id snapshot_created_after
```

Par exemple, la commande suivante affiche les index de blocs des blocs qui sont différents entre l'instantané `snap-09c9114207084f0d9` (celui que vous souhaitez archiver) et l'instantané `snap-024f49fe8dd853fa8` (créé après celui que vous souhaitez archiver).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-snapshot-id snap-024f49fe8dd853fa8
```

Voici la sortie de la commande, certains blocs étant omis.

```
{
  "BlockSize": 524288,
  "ChangedBlocks": [
    {
      "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
      "SecondBlockToken":
"ABgBASEvi9x80m7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
      "BlockIndex": 4
    },
    {
      "FirstBlockToken": "ABgBAeL0mtX6aBAAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
      "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLk0",
      "BlockIndex": 5
    },
    {
      "FirstBlockToken":
"ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
      "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrx0qGy4PKZ9SAAHaZ2HQBm9fQQU0+EXxQjVGv37",
      "BlockIndex": 13
    },
  ],
}
```

```

        "FirstBlockToken":
        "ABgBAbRlitCVI7c6hGsT4ckkKCw6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
        "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyv0wpozYII6UNCT",
        "BlockIndex": 14
    },
    {
        "FirstBlockToken": "ABgBAd+yxC026I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
        "SecondBlockToken": "ABgBACpPnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
        "BlockIndex": 18
    },
    ....
    {
        "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV031U/1KCW
+CTxF13cQ5p2f2h1njpuUiGbqKGUa",
        "BlockIndex": 13190
    },
    {
        "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ
+iSlWVpBIshmeyeS5FD/M0i64U+a9",
        "BlockIndex": 13191
    },
    {
        "SecondBlockToken": "ABgBAZ8DhMk+rR0Xa4dZ1NK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
        "BlockIndex": 13192
    },
    {
        "SecondBlockToken":
        "ABgBATH6MBVE90416sq0C27s1nVntFUpDwiMcRWGyJHy8sIgGL5yuYXHAvty",
        "BlockIndex": 13193
    },
    {
        "SecondBlockToken":
        "ABgBARuZykaFBWpCWrrJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn610Qyy+giN",
        "BlockIndex": 13194
    }
],
"ExpiryTime": 1637692677.286,
"VolumeSize": 8
}

```

6. Comparez la sortie renvoyée par les deux commandes lors de l'étape précédente. Si le même index de bloc apparaît dans les deux sorties de commande, cela indique que le bloc contient des données non référencées.

Par exemple, la sortie de commande de l'étape précédente indique que les blocs 4, 5, 13 et 14 sont uniques à l'instantané `snap-09c9114207084f0d9` et qu'ils ne sont référencés par aucun autre instantané dans la lignée des instantanés.

Pour déterminer la réduction du stockage de niveau standard, multipliez le nombre de blocs apparaissant dans les deux sorties de commande par 512 Kio, soit la taille du bloc d'instantané.

Par exemple, si 9 950 index de blocs apparaissent dans les deux sorties de commandes, cela indique que vous allez diminuer le stockage standard d'environ 4,85 GiB (9 950 blocs * 512 KiB = 4,85 GiB).

7. Déterminez les coûts de stockage liés au stockage des blocs non référencés dans le niveau standard pendant 90 jours. Comparez cette valeur au coût de stockage de l'instantané complet, décrit à l'étape 1, dans le niveau d'archivage. Vous pouvez déterminer vos économies de coûts en comparant les valeurs, en supposant que vous ne restaurez pas l'instantané complet à partir du niveau d'archivage pendant la période minimale de 90 jours. Pour de plus amples informations, veuillez consulter [Tarification et facturation pour l'archivage des instantanés Amazon EBS](#).

Autorisations IAM requises pour l'archivage des instantanés Amazon EBS

Par défaut, les utilisateurs ne sont pas autorisés à utiliser l'archivage des instantanés. Pour permettre aux utilisateurs d'utiliser l'archivage des instantanés, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Pour plus d'informations, consultez [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Pour utiliser l'archivage des instantanés, les utilisateurs ont besoin des autorisations suivantes.

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`
- `ec2:RestoreSnapshotTier`

Les utilisateurs de la console peuvent avoir besoin d'autorisations supplémentaires telles que `ec2:DescribeSnapshots`.

Pour archiver et restaurer des instantanés chiffrés, les AWS KMS autorisations supplémentaires suivantes sont requises.

- kms:CreateGrant
- kms:Decrypt
- kms:DescribeKey

Voici un exemple de politique IAM qui autorise les utilisateurs IAM à archiver, restaurer et afficher des instantanés chiffrés et non chiffrés. Elle inclut l'autorisation `ec2:DescribeSnapshots` pour les utilisateurs de la console. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

 Tip

Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour permettre à l'utilisateur de créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée pour le compte de l'utilisateur par un AWS service, comme illustré dans l'exemple suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSnapshotTierStatus",
      "ec2:ModifySnapshotTier",
      "ec2:RestoreSnapshotTier",
      "ec2:DescribeSnapshots",
      "kms:CreateGrant",
      "kms:Decrypt",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
```

```

        "kms:GrantIsForAWSResource": true
      }
    }
  }
}

```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Archiver un instantané Amazon EBS

Vous pouvez archiver n'importe quel instantané qui se trouve dans l'état `completed` et dont vous êtes propriétaire dans votre compte. Vous ne pouvez pas archiver les instantanés qui se trouvent dans l'état `pending` ou `error`, ou ceux qui sont partagés avec vous. Pour de plus amples informations, veuillez consulter [Considérations et limites relatives à l'archivage des instantanés Amazon EBS](#).

Si l'instantané est associé à une ou plusieurs AMI, vous devez d'abord désactiver ces AMI associées avant de pouvoir archiver l'instantané. Pour plus d'informations, voir [Désactiver une AMI](#).

Les instantanés archivés conservent leur identifiant de capture, leur état de chiffrement, leurs autorisations Gestion des identités et des accès AWS (IAM), les informations relatives au propriétaire et les balises de ressources. Toutefois, la restauration rapide d'instantané et le partage d'instantané sont automatiquement désactivés une fois celui-ci archivé.

Vous pouvez continuer à utiliser l'instantané pendant que l'archivage est en cours de traitement. Dès que l'état de hiérarchisation de l'instantané passe à `archival-complete`, vous ne pouvez plus l'utiliser.

Console

Pour archiver un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Dans la liste des instantanés, sélectionnez l'instantané à archiver, puis choisissez Actions, Archive snapshot (Archiver l'instantané).
4. Pour confirmer, choisissez Archive snapshot (Archiver l'instantané).

AWS CLI

Pour archiver un instantané

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-snapshot-tier.html> AWS CLI `modify-snapshot-tier`. Pour `--snapshot-id`, spécifiez l'ID de l'instantané à archiver. Pour `--storage-tier`, spécifiez `archive`.

```
aws ec2 modify-snapshot-tier \
  --snapshot-id snap-0abcdef1234567890 \
  --storage-tier archive
```

Voici un exemple de sortie. Le paramètre de `TieringStartTime` réponse indique la date et l'heure auxquelles le processus d'archivage a été démarré, au format horaire UTC (YYYY-MM-DDTHH:MM:SSZ).

```
{
  "SnapshotId": "snap-0abcdef1234567890",
  "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

PowerShell

Pour archiver un instantané

Utilisez l'applet de commande [Edit-EC2SnapshotTier](#). L'exemple suivant archive l'instantané spécifié.

```
Edit-EC2SnapshotTier `
  -SnapshotId snap-0abcdef1234567890 `
  -StorageTier "archive"
```

Restaurer un instantané Amazon EBS archivé

Avant de pouvoir utiliser un instantané archivé, vous devez d'abord le restaurer au niveau standard. L'instantané restauré possède les mêmes ID d'instantané, état de chiffrement, autorisations IAM, informations sur le propriétaire et identifications de ressources qu'avant son archivage. Une fois restauré, vous pouvez l'utiliser de la même manière que n'importe quel autre instantané de votre compte. L'instantané restauré est toujours un instantané complet.

Lorsque vous restaurez un instantané, vous pouvez choisir de le restaurer de façon permanente ou temporaire.

Si vous restaurez un instantané de façon permanente, il est déplacé définitivement du niveau d'archivage vers le niveau standard. L'instantané demeure restauré et prêt à être utilisé jusqu'à ce que vous le réarchiviez manuellement ou que vous le supprimiez manuellement. Lorsque vous restaurez définitivement un instantané, il est supprimé du niveau d'archivage.

Si vous restaurez temporairement un instantané, il est copié du niveau d'archivage vers le niveau standard pendant une période de restauration que vous spécifiez. L'instantané demeure restauré et prêt à être utilisé pendant la période de restauration uniquement. Pendant la période de restauration, une copie de l'instantané reste dans le niveau d'archivage. Une fois la période expirée, l'instantané est automatiquement supprimé du niveau standard. Vous pouvez augmenter ou diminuer la période de restauration ou changer le type de restauration pour le rendre permanent à tout moment pendant la période de restauration. Pour de plus amples informations, veuillez consulter [Modifier la période de restauration pour un instantané Amazon EBS temporairement restauré](#).

Si vous restaurez des instantanés associés à une AMI désactivée et que vous avez l'intention d'utiliser cette AMI, vous devez d'abord restaurer définitivement tous les instantanés associés, puis [réactiver une AMI désactivée](#) avant de pouvoir l'utiliser. Vous ne pouvez pas activer une AMI si les instantanés associés sont temporairement restaurés. Vous pouvez utiliser la commande suivante pour rechercher tous les instantanés associés à une AMI.

```
aws ec2 describe-images --image-id ami_id \
```

```
--query Images[*].BlockDeviceMappings[*].Ebs[*].SnapshotId[]
```

Console

Pour restaurer un instantané à partir de l'archive

Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

1. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
2. Dans la liste des instantanés, sélectionnez l'instantané à archiver, puis choisissez Actions, Restore snapshot (Restaurer l'instantané).
3. Spécifiez le type de restauration à effectuer. Pour Restore type (Type de restauration), effectuez l'une des opérations suivantes :
 - Pour restaurer définitivement l'instantané, sélectionnez Permanent.
 - Pour restaurer temporairement l'instantané, sélectionnez Temporary (Temporaire), puis pour Temporary restore period (Période de restauration temporaire), saisissez le nombre de jours de restauration de l'instantané.
4. Pour confirmer, choisissez Restore snapshot (Restaurer l'instantané).

AWS CLI

Pour restaurer définitivement un instantané archivé

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-snapshot-tier.html> AWS CLI restore-snapshot-tier avec l'option. --permanent-restore Pour --snapshot-id, spécifiez l'ID de l'instantané à restaurer.

```
aws ec2 restore-snapshot-tier \  
  --snapshot-id snap-0abcdef1234567890 \  
  --permanent-restore
```

Voici un exemple de sortie.

```
{  
  "SnapshotId": "snap-0abcdef1234567890",  
  "IsPermanentRestore": true  
}
```


Pour restaurer temporairement un instantané archivé

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-snapshot-tier.html> AWS CLI `restore-snapshot-tier`. Omettez l'option `--permanent-restore`. Pour `--temporary-restore-days`, spécifiez le nombre de jours pendant lesquels vous souhaitez restaurer le snapshot. La plage autorisée est comprise entre 1 et 180 jours. Si vous ne spécifiez aucune valeur, la valeur par défaut est 1 jour.

L'exemple suivant restaure temporairement l'instantané spécifié pendant une période de restauration de 5 jours.

```
aws ec2 restore-snapshot-tier \  
  --snapshot-id snap-0abcdef1234567890 \  
  --temporary-restore-days 5
```

Voici un exemple de sortie.

```
{  
  "SnapshotId": "snap-0abcdef1234567890",  
  "RestoreDuration": 5,  
  "IsPermanentRestore": false  
}
```

PowerShell

Pour restaurer définitivement un instantané archivé

Utilisez l'applet de commande [Restore-EC2SnapshotTier](#).

```
Restore-EC2SnapshotTier `  
  -SnapshotId snap-0abcdef1234567890 `  
  -PermanentRestore $true
```

Pour restaurer temporairement un instantané archivé

Utilisez l'applet de commande [Restore-EC2SnapshotTier](#).

```
Restore-EC2SnapshotTier `  
  -SnapshotId snap-0abcdef1234567890 `
```

-TemporaryRestoreDays 5

Modifier la période de restauration pour un instantané Amazon EBS temporairement restauré

Lorsque vous restaurez temporairement un instantané, vous devez spécifier le nombre de jours pendant lesquels l'instantané doit rester restauré dans votre compte. Une fois la période expirée, l'instantané est automatiquement supprimé du niveau standard.

Vous pouvez modifier la période de restauration d'un instantané temporairement restauré à tout moment.

Vous pouvez choisir d'augmenter ou de diminuer la période de restauration, ou de changer le type de restauration de type temporaire à permanent.

Si vous modifiez la période de restauration, la nouvelle période de restauration est effective à partir de la date actuelle. Par exemple, si vous spécifiez une nouvelle période de restauration de 5 jours, l'instantané restera restauré pendant cinq jours à compter de la date actuelle.

Note

Vous pouvez mettre fin prématurément à une restauration temporaire en fixant la période de restauration à 1 jour.

Si vous changez le type de restauration de temporaire à permanent, la copie de l'instantané est supprimée du niveau d'archivage et l'instantané reste disponible dans votre compte jusqu'à ce que vous le réarchiviez ou que vous le supprimiez manuellement.

Console

Pour modifier la période de restauration ou le type de restauration

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Dans la liste des instantanés, sélectionnez l'instantané à archiver, puis choisissez Actions, Restore snapshot from archive (Restaurer l'instantané depuis une archive).
4. Pour Restore type (Type de restauration), effectuez l'une des opérations suivantes :

- Pour passer du type de restauration temporaire à permanent, sélectionnez Permanent.
 - Pour augmenter ou diminuer la période de restauration, conservez Temporary (Temporaire), puis pour Temporary restore period (Période de restauration temporaire), saisissez la nouvelle période de restauration en jours.
5. Pour confirmer, choisissez Restore snapshot (Restaurer l'instantané).

AWS CLI

Pour modifier la période de restauration ou le type de restauration

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/restore-snapshot-tier.html> restore-snapshot-tier. Pour --snapshot-id, spécifiez l'ID de l'instantané que vous avez précédemment temporairement restauré. Pour passer du type de restauration temporaire à permanent, spécifiez --permanent-restore et omettez --temporary-restore-days. Pour augmenter ou diminuer la période de restauration, omettez --permanent-restore et pour --temporary-restore-days, spécifiez la nouvelle période de restauration en jours.

Exemple : augmenter ou diminuer la période de restauration

La commande suivante modifie la période de restauration de l'instantané spécifié en 10 jours.

```
aws ec2 restore-snapshot-tier \
  --snapshot-id snap-0abcdef1234567890 \
  --temporary-restore-days 10
```

Voici un exemple de sortie.

```
{
  "SnapshotId": "snap-0abcdef1234567890",
  "RestoreDuration": 10,
  "IsPermanentRestore": false
}
```

Exemple : changer le type de restauration en mode permanent

La commande suivante change le type de restauration de l'instantané spécifié de temporaire à permanent.

```
aws ec2 restore-snapshot-tier \  
  --snapshot-id snap-0abcdef1234567890 \  
  --permanent-restore
```

Voici un exemple de sortie.

```
{  
  "SnapshotId": "snap-0abcdef1234567890",  
  "IsPermanentRestore": true  
}
```

PowerShell

Pour modifier la période de restauration ou le type de restauration

Utilisez l'applet de commande [Restore-EC2SnapshotTier](#). Pour -SnapshotId, spécifiez l'ID de l'instantané que vous avez précédemment temporairement restauré. Pour passer du type de restauration temporaire à permanent, spécifiez -PermanentRestore et omettez -TemporaryRestoreDays. Pour augmenter ou diminuer la période de restauration, omettez -PermanentRestore et pour -TemporaryRestoreDays, spécifiez la nouvelle période de restauration en jours.

Exemple : augmenter ou diminuer la période de restauration

La commande suivante modifie la période de restauration de l'instantané spécifié en 10 jours.

```
Restore-EC2SnapshotTier `  
  -SnapshotId snap-0abcdef1234567890 `  
  -TemporaryRestoreDays 10
```

Exemple : changer le type de restauration en mode permanent

La commande suivante change le type de restauration de l'instantané spécifié de temporaire à permanent.

```
Restore-EC2SnapshotTier `  
  -SnapshotId snap-0abcdef1234567890 `  
  -PermanentRestore $true
```

Afficher les instantanés Amazon EBS archivés

Console

Pour afficher les informations de niveau de stockage pour un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Dans la liste des instantanés, sélectionnez l'instantané et choisissez l'onglet Storage tier (Niveau de stockage).

L'onglet fournit les informations suivantes :

- Last tier change started on (Dernier changement de niveau démarré le) : date et heure auxquelles la dernière archive ou restauration a démarré.
- Tier change progress (Progrès du changement de niveau) : la progression de la dernière action d'archivage ou de restauration, sous forme de pourcentage.
- Storage tier (Niveau de stockage) : niveau de stockage de l'instantané. Toujours archive pour les instantanés archivés, et standard pour les instantanés stockés sur le niveau standard, y compris les instantanés temporairement restaurés.
- Tiering status (Statut de hiérarchisation) : état de la dernière action d'archivage ou de restauration.
- Archive completed on (Archivage terminée le) : date et heure auxquelles l'archivage s'est terminé.
- Temporary restore expires on (La restauration temporaire expire le) : date et heure auxquelles un instantané restauré temporairement doit expirer.

AWS CLI

Pour afficher les informations d'archivage relatives à un instantané archivé

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-snapshot-tier-status.html> describe-snapshot-tier-status. Spécifiez le filtre snapshot-id et pour la valeur du filtre, spécifiez l'ID de l'instantané. Pour afficher tous les instantanés archivés, vous pouvez également omettre le filtre.

```
--filters "Name=snapshot-id, Values=snapshot_id"
```

La sortie comprend les paramètres de réponse suivants :

- **Status** : état de l'instantané. Toujours `completed` pour les instantanés archivés. Seuls les instantanés qui sont dans l'état `completed` peuvent être archivés.
- **LastTieringStartTime**— La date et l'heure auxquelles le processus d'archivage a commencé, au format horaire UTC (YYYY-MM-DDTHH:MM:SSZ).
- **LastTieringOperationState** : état actuel du processus d'archivage. Les états possibles incluent : `archival-in-progress` | `archival-completed` | `archival-failed` | `permanent-restore-in-progress` | `permanent-restore-completed` | `permanent-restore-failed` | `temporary-restore-in-progress` | `temporary-restore-completed` | `temporary-restore-failed`
- **LastTieringProgress** : progression du processus d'archivage des instantanés, sous forme de pourcentage.
- **StorageTier** : niveau de stockage de l'instantané. Toujours `archive` pour les instantanés archivés, et `standard` pour les instantanés stockés sur le niveau standard, y compris les instantanés temporairement restaurés.
- **ArchivalCompleteTime**— La date et l'heure auxquelles le processus d'archivage s'est terminé, au format UTC (YYYY-MM-DDTHH:MM:SSZ).

Exemple : Décrire un instantané

L'exemple suivant affiche des informations sur le cliché spécifié.

```
aws ec2 describe-snapshot-tier-status \
  --filters "Name=snapshot-id, Values=snap-0abcdef1234567890"
```

Voici un exemple de sortie.

```
{
  "SnapshotTierStatuses": [
    {
      "Status": "completed",
      "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
      "LastTieringProgress": 100,
      "Tags": [],
      "VolumeId": "vol-01234567890abcdef",
      "LastTieringOperationState": "archival-completed",
      "StorageTier": "archive",
    }
  ]
}
```

```

        "OwnerId": "123456789012",
        "SnapshotId": "snap-0abcdef1234567890",
        "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
      }
    ]
  }

```

Pour afficher les instantanés de niveau standard et archivés

Utilisez la commande [describe-snapshots](#). Pour `--snapshot-ids`, spécifiez l'ID de l'instantané.

```
aws ec2 describe-snapshots --snapshot-ids snap-0abcdef1234567890
```

Voici un exemple de sortie. Le paramètre de réponse `StorageTier` indique si l'instantané est actuellement archivé. `archive` indique que l'instantané est actuellement archivé et stocké dans le niveau d'archivage, et `standard` indique que l'instantané n'est actuellement pas archivé et qu'il est stocké dans le niveau standard.

Dans l'exemple de sortie suivant, seul Snap A est archivé. Snap B et Snap C ne le sont pas.

En outre, le paramètre de réponse `RestoreExpiryTime` est renvoyé uniquement pour les instantanés temporairement restaurés à partir de l'archive. Il indique la date à laquelle les instantanés restaurés temporairement doivent être automatiquement retirés du niveau standard. Il n'est pas renvoyé pour les instantanés qui sont restaurés de façon permanente.

Dans l'exemple suivant, la sortie Snap C est temporairement restaurée et sera automatiquement supprimée du niveau standard le 19/09/2021 T21:00:00.000Z (19 septembre 2021 à 21h00 UTC).

```

{
  "Snapshots": [
    {
      "Description": "Snap A",
      "Encrypted": false,
      "VolumeId": "vol-01234567890aaaaaa",
      "State": "completed",
      "VolumeSize": 8,
      "StartTime": "2021-09-07T21:00:00.000Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "SnapshotId": "snap-01234567890aaaaaa",
      "StorageTier": "archive",
      "Tags": []
    }
  ]
}

```

```

    },
    {
      "Description": "Snap B",
      "Encrypted": false,
      "VolumeId": "vol-09876543210bbbbbb",
      "State": "completed",
      "VolumeSize": 10,
      "StartTime": "2021-09-14T21:00:00.000Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "SnapshotId": "snap-09876543210bbbbbb",
      "StorageTier": "standard",
      "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
      "Tags": []
    },
    {
      "Description": "Snap C",
      "Encrypted": false,
      "VolumeId": "vol-054321543210cccccc",
      "State": "completed",
      "VolumeSize": 12,
      "StartTime": "2021-08-01T21:00:00.000Z",
      "Progress": "100%",
      "OwnerId": "123456789012",
      "SnapshotId": "snap-054321543210cccccc",
      "StorageTier": "standard",
      "Tags": []
    }
  ]
}

```

Pour afficher uniquement les instantanés stockés dans le niveau d'archivage ou le niveau standard

Utilisez la commande [describe-snapshots](#). Incluez l'option `--filter`, avec le nom du filtre `storage-tier`. Pour la valeur du filtre, spécifiez `archive` soit `standard`. L'exemple suivant affiche uniquement les instantanés archivés.

```
aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

PowerShell

Pour afficher les informations d'archivage d'un instantané archivé

Utilisez l'applet de commande [Get-EC2SnapshotTierStatus](#).

```
Get-EC2SnapshotTierStatus `
  -Filter @{{Name="snapshot-id"; Values="snap-0abcdef1234567890"}}
```

Pour afficher les instantanés de niveau standard et archivés

Utilisez l'applet de commande [Get-EC2Snapshot](#).

```
Get-EC2Snapshot `
  -SnapshotId snap-0abcdef1234567890
```

Pour afficher uniquement les instantanés stockés dans le niveau d'archivage ou le niveau standard

Utilisez l'applet de commande [Get-EC2Snapshot](#). L'exemple suivant affiche uniquement les instantanés archivés.

```
Get-EC2Snapshot `
  -Filter @{{Name="storage-tier"; Values="archive"}}
```

Surveillez l'archivage des instantanés Amazon EBS à l'aide d'événements CloudWatch

Amazon EBS émet des événements liés aux actions d'archivage des instantanés. Vous pouvez utiliser AWS Lambda Amazon CloudWatch Events pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur [Amazon](#).

Les événements suivants sont disponibles :

- `archiveSnapshot` : émis lorsqu'une action d'archivage d'un instantané réussit ou échoue.

Voici un exemple d'événement émis lorsqu'une action d'archivage d'instantané réussit.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
```

```

"time": "2021-05-25T13:12:22Z",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
],
"detail": {
  "event": "archiveSnapshot",
  "result": "succeeded",
  "cause": "",
  "request-id": "123456789",
  "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
  "startTime": "2021-05-25T13:12:22Z",
  "endTime": "2021-05-45T15:30:00Z",
  "recycleBinExitTime": "2021-10-45T15:30:00Z"
}

```

Voici un exemple d'événement émis lorsqu'une action d'archivage d'instantané échoue.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}

```

- **permanentRestoreSnapshot** : émis lorsqu'une action de restauration permanente réussit ou échoue.

Voici un exemple d'événement émis lorsqu'une action de restauration permanente réussit.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}
```

Voici un exemple d'événement émis lorsqu'une action de restauration permanente échoue.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
  }
}
```

```

    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}

```

- **temporaryRestoreSnapshot** : émis lorsqu'une action de restauration permanente réussit ou échoue.

Voici un exemple d'événement émis lorsqu'une action de restauration temporaire réussit.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}

```

Voici un exemple d'événement émis lorsqu'une action de restauration temporaire échoue.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",

```

```

"account": "123456789012",
"time": "2021-05-25T13:12:22Z",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
],
"detail": {
  "event": "temporaryRestoreSnapshot",
  "result": "failed",
  "cause": "Source snapshot ID is not valid",
  "request-id": "1234567890",
  "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
  "startTime": "2021-05-25T13:12:22Z",
  "endTime": "2021-05-45T15:30:00Z",
  "recycleBinExitTime": "2021-10-45T15:30:00Z"
}
}

```

- **restoreExpiry** : émis lorsque la période de restauration d'un instantané temporairement restauré expire.

Voici un exemple.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "restoryExpiry",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}

```

```
}  
}
```

Supprimer un instantané Amazon EBS

Une fois que vous n'avez plus besoin d'un instantané Amazon EBS d'un volume, vous pouvez le supprimer. La suppression d'un instantané n'a aucun effet sur le volume. La suppression d'un volume n'a aucun effet sur les instantanés créés à partir de celui-ci.

Rubriques

- [Considérations relatives à la suppression des instantanés](#)
- [Comment fonctionne la suppression de captures d'écran incrémentielles](#)
- [Suppression d'un instantané](#)
- [Supprimer des instantanés multivolumes](#)

Considérations relatives à la suppression des instantanés

Les considérations suivantes s'appliquent à la suppression des instantanés :

- Vous ne pouvez pas supprimer un instantané de l'appareil racine d'un volume EBS utilisé par une AMI enregistrée. Cette considération s'applique même si l'AMI enregistrée est obsolète ou désactivée. Vous devez commencer par annuler l'inscription de l'AMI avant de pouvoir supprimer l'instantané. Pour plus d'informations, consultez [Désenregistrer votre AMI](#).
- Vous ne pouvez pas supprimer un instantané géré par le AWS Backup service à l'aide d'Amazon EC2. Utilisez-le plutôt AWS Backup pour supprimer les points de restauration correspondants dans le coffre-fort de sauvegarde. Pour plus d'informations, consultez [Suppression des sauvegardes](#) dans le Guide du développeur AWS Backup .
- Vous pouvez créer, conserver et supprimer les instantanés manuellement, ou vous pouvez utiliser Amazon Data Lifecycle Manager pour les gérer à votre place. Pour plus d'informations, consultez [Amazon Data Lifecycle Manager](#).
- Même si vous pouvez supprimer un instantané qui est toujours en cours, l'instantané doit être terminé avant que la suppression prenne effet. Cela pourrait prendre beaucoup de temps. En outre, si vous avez atteint votre limite d'instantanés simultanés et que vous tenez de prendre un instantané supplémentaire, vous pouvez obtenir une erreur

ConcurrentSnapshotLimitExceeded. Pour plus d'informations, consultez les quotas [de service](#) pour Amazon EBS dans le Référence générale d'Amazon Web Services.

- Si vous supprimez un instantané qui correspond à une règle de conservation de la corbeille, l'instantané est conservé dans la corbeille au lieu d'être immédiatement supprimé. Pour plus d'informations, voir [Corbeille](#).
- Vous ne pouvez pas supprimer les instantanés associés à des EBS-backed AMI désactivées. Pour plus d'informations, voir [Désactiver une AMI](#).
- Vous ne pouvez pas supprimer les instantanés qui sont partagés avec vous.
- Si vous supprimez un instantané partagé qui vous appartient, tous les comptes avec lesquels il est partagé n'y ont plus accès.

Comment fonctionne la suppression de captures d'écran incrémentielles

Si vous effectuez régulièrement des instantanés d'un volume, les instantanés sont incrémentiels. Cela signifie que seuls les blocs qui ont changé sur l'appareil depuis le dernier instantané sont enregistrés dans le nouvel instantané. Bien que les instantanés soient enregistrés de manière incrémentielle, le processus de suppression de l'instantané prévoit que vous ayez uniquement besoin de conserver l'instantané le plus récent pour créer le volume.

Si des données étaient présentes sur un volume stocké dans un instantané ou une série d'instantanés précédents et que ces données sont supprimées ultérieurement de ce volume, elles sont toujours considérées comme des données uniques d'instantanés antérieurs. Les données uniques sont uniquement supprimées de la séquence d'instantanés si tous les instantanés qui référencent les données uniques sont supprimés.

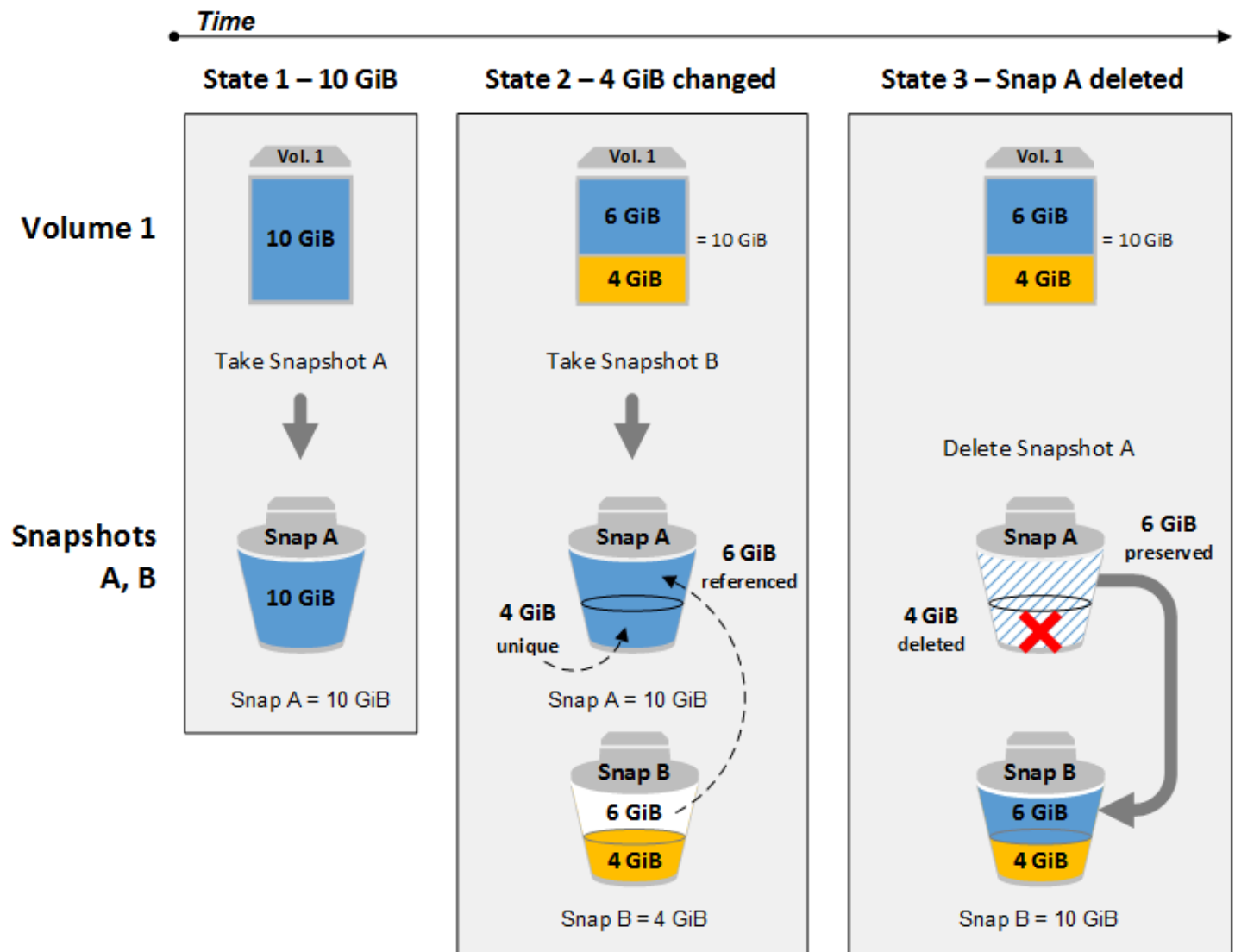
Lorsque vous supprimez un instantané, seules les données référencées exclusivement par cet instantané sont supprimées. Les données uniques ne sont supprimées que si tous les instantanés qui les référencent sont supprimés. La suppression d'instantanés précédents d'un volume n'a aucune répercussion sur votre capacité à créer des volumes à partir d'instantanés ultérieurs de ce même volume.

La suppression d'un instantané ne réduit pas les coûts de stockage des données de votre organisation. D'autres instantanés peuvent faire référence aux données de cet instantané et les données référencées sont toujours conservées. Si vous supprimez un instantané contenant des données utilisées par un instantané ultérieur, les coûts associés aux données référencées sont alloués à l'instantané ultérieur. Pour plus d'informations sur la façon dont les instantanés stockent les données, consultez [Comment fonctionnent les instantanés Amazon EBS](#) et l'exemple ci-dessous.

Dans le graphique suivant, Volume 1 est affiché à trois moments différents. Un instantané a capturé chacun des deux premiers états, et dans le troisième, un instantané a été supprimé.

- À l'état 1, le volume contient 10 GiB de données. Comme Snap A est le premier instantané pris du volume, la totalité des 10 Go de données doit être copiée. Dans cet état, le stockage de 10 Go de données d'instantanés vous est facturé.
- À l'état 2, le volume contient toujours 10 GiB de données, mais 4 GiB ont changé. Snap B ne stocke que les 4 GiB qui ont changé après la prise du Snap A, et il fait référence aux 6 GiB de données inchangées qui sont déjà stockées dans Snap A. Dans cet état, vous êtes facturé pour le stockage de 14 GiB de données de snapshot (10 Go pour Snap A + 4 GiB pour Snap B).
- À l'état 3, le volume reste inchangé mais le Snap A est supprimé. Étant donné que les 6 Go de données inchangées du Snap A sont toujours référencés par Snap B, ces données sont conservées et associées à Snap B. Les 4 GiB de données uniques du Snap A sont supprimés car elles ne sont plus référencées par les autres instantanés. Dans cet état, vous êtes facturé pour le stockage de 10 Go de données d'instantané (6 Go de données conservées dans le Snap A + 4 GiB de données dans le Snap B).

Suppression d'un instantané avec certaines de ses données référencées par un autre instantané



Suppression d'un instantané

Console

Pour supprimer un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané.
4. Choisissez Actions, Delete snapshot (Supprimer un instantané).
5. Lorsque vous êtes invité à confirmer, entrez **delete**, puis choisissez Delete (Supprimer).

AWS CLI

Pour supprimer un instantané

Utilisez la commande [delete-snapshot](#).

```
aws ec2 delete-snapshot --snapshot-id snap-0abcdef1234567890
```

PowerShell

Pour supprimer un instantané

Utilisez l'applet de commande [Remove-EC2Snapshot](#).

```
Remove-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

Conseil pour la résolution de problèmes

Si un message `Failed to delete snapshot` d'erreur indique que l'instantané est actuellement utilisé par une AMI, vous devez [désenregistrer l'AMI associée](#) avant de pouvoir supprimer le cliché. Vous ne pouvez pas supprimer les instantanés associés à une AMI. Si vous utilisez la console et que l'AMI associée est désactivée, vous devez sélectionner le filtre `Images désactivées` sur l'écran des AMI pour afficher les AMI désactivées.

Supprimer des instantanés multivolumes

Pour supprimer des instantanés multi-volumes, récupérez tous les instantanés de votre ensemble multi-volume en utilisant l'étiquette que vous avez appliquée à l'ensemble lorsque vous avez créé les instantanés. Ensuite, supprimez individuellement les instantanés.

Vous ne vous verrez pas empêché de supprimer des instantanés individuels dans l'ensemble d'instantanés multi-volumes. Si vous supprimez un instantané alors qu'il se trouve à l'état `pending state`, seul cet instantané est supprimé. Les autres instantanés de l'ensemble d'instantanés multi-volumes sont toujours terminés avec succès.

Restauration d'instantané rapide Amazon EBS

La restauration d'instantané rapide (FSR) Amazon EBS vous permet de créer un volume à partir d'un instantané entièrement initialisé à la création. Cela permet d'éliminer la latence I/O des opérations sur un bloc lors de son premier accès. Les volumes créés avec la restauration rapide d'instantané fournissent instantanément la totalité des performances allouées.

Pour commencer, activez la restauration d'instantané rapide pour des instantanés spécifiques dans des zones de disponibilité déterminées. Chaque paire d'instantanés/zones de disponibilité fait référence à une seule restauration d'instantané rapide. Lorsque vous créez un volume à partir d'un de ces instantanés dans l'une de ses zones de disponibilité activées, le volume est restauré à l'aide de la restauration d'instantané rapide.

Vous devez activer explicitement la restauration rapide des instantanés pour chaque instantané. Par exemple, si vous créez un nouvel instantané à partir d'un volume qui a été restauré à partir d'un instantané activé pour la restauration rapide des instantanés, le nouveau cliché n'est pas automatiquement activé pour la restauration rapide des instantanés. Si vous copiez un instantané qui est activé pour la restauration rapide des instantanés, la copie des instantanés n'est pas automatiquement activée pour la restauration rapide des instantanés.

Le nombre de volumes que vous pouvez restaurer avec la totalité des bénéfices en matière de performance de la fonction de restauration d'instantané rapide est déterminé par les crédits de création de volume associés à l'instantané. Pour plus d'informations, consultez [Crédits de création de volumes Amazon EBS Fast Snapshot Restore](#).

Vous pouvez activer la restauration d'instantané rapide pour les instantanés que vous possédez et pour les instantanés publics et privés qui sont partagés avec vous.

Table des matières

- [Considérations](#)
- [Tarification et facturation](#)
- [Crédits de création de volumes Amazon EBS Fast Snapshot Restore](#)
- [Configurer la restauration rapide des instantanés pour un instantané Amazon EBS](#)
- [Vérifiez l'état de restauration rapide d'un instantané Amazon EBS](#)
- [Afficher les volumes Amazon EBS restaurés à l'aide de la restauration rapide des instantanés](#)

Considérations

- La restauration rapide des instantanés n'est pas prise en charge avec AWS Outposts les zones locales et les zones de longueur d'onde.
- La restauration rapide des instantanés peut être activée sur des instantanés d'une taille inférieure ou égale à 16 TiO.
- Les volumes provisionnés avec des performances allant jusqu'à 64 000 IOPS et 1 000 MiB/s débits bénéficient de tous les avantages en termes de performances d'une restauration rapide des snapshots. Pour les volumes provisionnés dont les performances sont supérieures à 64 000 IOPS ou à 1 000 MiB/s débits, nous vous recommandons d'[initialiser le volume](#) pour bénéficier de toutes ses performances.
- Vous pouvez activer jusqu'à 5 instantanés pour une restauration d'instantané rapide par région. Le quota s'applique aux instantanés que vous possédez et aux instantanés qui sont partagés avec vous. Si vous activez la restauration d'instantané rapide pour un instantané partagé avec vous, elle est comptabilisée dans votre quota de restauration d'instantané rapide. Elle n'est pas comptabilisée dans le quota de restauration rapide du propriétaire de l'instantané.
- Amazon EBS émet des CloudWatch événements Amazon lorsque l'état de restauration rapide d'un instantané change. Pour de plus amples informations, veuillez consulter [Événements de restauration d'instantané rapide EBS](#).

Tarification et facturation

Vous êtes facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée pour un instantané dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure.

Par exemple, si vous activez la restauration d'instantané rapide pour un instantané dans US-East-1a pendant un mois (30 jours), vous êtes facturé 540 USD (1 instantané x 1 AZ x 720 heures x \$0.75 par heure). Si vous activez la restauration d'instantané rapide pour deux instantanés dans us-east-1a, us-east-1b et us-east-1c pour la même période, vous êtes facturé 3 240 \$ (2 instantanés x 3 AZs x 720 heures x \$0.75 par heure).

Si vous activez la restauration d'instantané rapide pour un instantané public ou privé partagé avec vous, votre compte est facturé ; le propriétaire de l'instantané ne l'est pas. Lorsqu'un instantané partagé avec vous est supprimé ou non partagé par son propriétaire, la restauration d'instantané rapide est désactivée pour l'instantané dans votre compte et la facturation est arrêtée.

Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

Crédits de création de volumes Amazon EBS Fast Snapshot Restore

Le nombre de volumes qui reçoivent la totalité des bénéfices en matière de performances de la fonction de restauration d'instantané rapide est déterminé par les crédits de création de volume associés à l'instantané. Il y a un compartiment de crédits par instantané et par zone de disponibilité. Chaque volume que vous créez à partir d'un instantané pour lequel la fonction de restauration d'instantané rapide est activée consomme un crédit du compartiment de crédits. Vous devez disposer d'au moins un crédit dans le compartiment pour créer un volume initialisé à partir de l'instantané. Si vous créez un volume mais qu'il y a moins d'un crédit dans le compartiment, le volume est créé sans bénéficier d'une restauration d'instantané rapide.

Lorsque vous activez la restauration d'instantané rapide pour un instantané partagé avec vous, vous obtenez un compartiment de crédit distinct pour l'instantané partagé dans votre compte. Si vous créez des volumes à partir de l'instantané partagé, les crédits sont consommés à partir de votre compartiment de crédit ; ils ne sont pas consommés à partir du compartiment de crédit du propriétaire de l'instantané.

La taille de la tranche de crédits et le taux de recharge sont basés sur la taille de l'instantané (qui est également la taille du volume source), et non sur la taille des données de l'instantané. Par exemple, si vous créez un instantané à partir d'un volume de 200 Go contenant 150 Go de données et que vous l'activez pour une restauration rapide des instantanés, la taille du compartiment de crédits et le taux de recharge sont basés sur 200 GiB.

Lorsque vous activez la restauration d'instantané rapide pour un instantané, le compartiment de crédits ne contient aucun crédit au départ et se recharge à une vitesse définie jusqu'à ce qu'il atteigne sa capacité de crédits maximale. De plus, au fur et à mesure que vous consommez des crédits, le compartiment de crédits se recharge jusqu'à ce qu'il atteigne sa capacité de crédits maximale.

La vitesse de rechargement de chaque compartiment de crédits est calculée comme suit :

$$\text{MIN} (10, (1024 \div \text{snapshot_size_gib}))$$

Et la taille du compartiment de crédits est calculée comme suit :

$$\text{MAX} (1, \text{MIN} (10, (1024 \div \text{snapshot_size_gib})))$$

Par exemple, si vous activez la restauration d'instantané rapide pour un instantané d'une taille de 128 GiB, la vitesse de rechargement est de 0.1333 crédits par minute.

```
MIN (10, (1024 ÷ 128))  
= MIN (10, 8)  
= 8 credits per hour  
= 0.1333 credits per minute
```

Et la taille maximale du compartiment de crédits est de 8 crédits.

```
MAX (1, MIN (10, (1024 ÷ 128)))  
= MAX (1, MIN (10, 8))  
= MAX (1, 8)  
= 8 credits
```

Dans cet exemple, lorsque vous activez la restauration d'instantané rapide, le compartiment de crédits ne contient aucun crédit au départ. Après 8 minutes, le compartiment de crédits dispose de suffisamment de crédits pour créer un volume initialisé (0.1333 credits × 8 minutes = 1.066 credits). Lorsque le compartiment de crédits est plein, vous pouvez créer simultanément 8 volumes initialisés (8 crédits). Lorsque le compartiment est en dessous de sa capacité maximale, il se recharge à une vitesse de 0.1333 crédits par minute.

Vous pouvez utiliser CloudWatch des statistiques pour surveiller la taille de vos tranches de crédits et le nombre de crédits disponibles dans chaque tranche. Pour de plus amples informations, veuillez consulter [Métriques de restauration d'instantané rapide](#).

Après que vous avez créé un volume à partir d'un instantané avec la fonction de restauration d'instantané rapide activée, vous pouvez décrire le volume à l'aide de [describe-volumes](#) et vérifier le champ `fastRestored` et la sortie pour déterminer si le volume a été créé comme volume initialisé à l'aide de la restauration d'instantané rapide.

Configurer la restauration rapide des instantanés pour un instantané Amazon EBS

La restauration d'instantané rapide est désactivée par défaut pour un instantané. Vous pouvez activer ou désactiver la restauration d'instantané rapide pour les instantanés que vous possédez et pour ceux qui sont partagés avec vous. Lorsque vous activez ou désactivez la restauration d'instantané rapide pour un instantané, les modifications s'appliquent uniquement à votre compte.

 Note

Lorsque vous activez la restauration d'instantané rapide pour un instantané, votre compte est facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure.

Lorsque vous supprimez un instantané que vous possédez, la restauration d'instantané rapide est automatiquement désactivée pour cet instantané dans votre compte. Si vous avez activé la restauration d'instantané rapide pour un instantané partagé avec vous et que le propriétaire de l'instantané le supprime ou l'annule, la restauration d'instantané rapide est automatiquement désactivée pour l'instantané partagé dans votre compte.

Si vous avez activé la restauration rapide d'instantané pour un instantané partagé avec vous et que celui-ci est chiffré à l'aide d'une clé CMK personnalisée, la restauration rapide d'instantané n'est pas automatiquement désactivée pour l'instantané lorsque le propriétaire de ce dernier révoque votre accès à la clé CMK personnalisée. Vous devez désactiver manuellement la restauration d'instantané rapide pour cet instantané.

Après avoir activé la restauration rapide d'instantané pour un instantané, il passe à l'état `optimizing`. Les instantanés qui ont l'état `optimizing` offrent certains avantages en termes de performances lors de leur utilisation pour restaurer des volumes. Ils commencent à fournir tous les avantages de performances de la restauration d'instantané rapide uniquement après leur passage à l'état `enabled`.

Console

Pour configurer la restauration rapide des instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Sélectionnez l'instantané, puis choisissez Actions, Manage fast snapshot restore (Gérer la restauration d'instantané rapide).
4. La section Paramètres de restauration rapide d'instantané répertorie toutes les zones de disponibilité dans lesquelles vous pouvez activer la restauration rapide des instantanés pour l'instantané sélectionné. Le paramètre de volume Current status (État actuel) indique si la restauration d'instantané rapide est actuellement activée ou désactivée pour chaque zone.

Pour activer la restauration d'instantané rapide dans une zone où elle est actuellement désactivée, sélectionnez la zone, choisissez Enable (Activer), puis pour confirmer, choisissez Enable (Activer).

Pour désactiver la restauration d'instantané rapide dans une zone où elle est actuellement activée, sélectionnez la zone, puis choisissez Disable (Désactiver).

5. Lorsque vous avez apporté les modifications requises, choisissez Close (Fermer).

AWS CLI

Pour activer la restauration rapide d'un instantané

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/enable-fast-snapshot-restores.html> enable-fast-snapshot-restore.

```
aws ec2 enable-fast-snapshot-restores \
  --availability-zones us-east-1a us-east-1b \
  --source-snapshot-ids snap-0abcdef1234567890
```

Pour désactiver la restauration rapide d'instantané

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/disable-fast-snapshot-restores.html> disable-fast-snapshot-restore.

```
aws ec2 disable-fast-snapshot-restores \
  --availability-zones us-east-1a \
  --source-snapshot-ids snap-0abcdef1234567890
```

L'exemple suivant utilise la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-fast-snapshot-restores.html> describe-fast-snapshot-restore pour décrire vos restaurations rapides d'instantanés désactivés.

```
aws ec2 describe-fast-snapshot-restores \
  --filters Name=state,Values=disabled
```

PowerShell

Pour activer la restauration rapide d'un instantané

Utilisez l'applet de commande [Enable-EC2FastSnapshotRestore](#).


```
Enable-EC2FastSnapshotRestore `
  -AvailabilityZone us-east-1a us-east-1b `
  -SourceSnapshotId snap-0abcdef1234567890
```

Pour désactiver la restauration rapide d'instantané

Utilisez l'applet de commande [Disable-EC2FastSnapshotRestore](#).

```
Disable-EC2FastSnapshotRestore `
  -AvailabilityZone us-east-1a `
  -SourceSnapshotId snap-0abcdef1234567890
```

L'exemple suivant utilise l'[Get-EC2FastSnapshotRestore](#) applet de commande pour décrire vos restaurations rapides de snapshots désactivées.

```
Get-EC2FastSnapshotRestore `
  -Filter @{Name="state"; Values="disabled"}
```

Vérifiez l'état de restauration rapide d'un instantané Amazon EBS

La restauration d'instantané rapide pour un instantané peut être dans l'un des états suivants.

- **enabling** — Une demande d'activation de la fonction de restauration d'instantané rapide a été effectuée.
- **optimizing** — La fonction de restauration d'instantané rapide est en cours d'activation. L'optimisation d'un instantané prend 60 minutes par Tio. Les instantanés dans cet état offrent quelques avantages en termes de performances lors de la restauration de volumes.
- **enabled** — La fonction de restauration d'instantané rapide est activée. Les instantanés qui affichent cet état et qui disposent de suffisamment de crédits de création de volume offrent tous les avantages en termes de performances lors de la restauration de volumes.
- **disabling** — Une demande de désactivation de la fonction de restauration d'instantané rapide a été faite ou une demande d'activation de la fonction de restauration d'instantané rapide a échoué.
- **disabled** — La fonction de restauration d'instantané rapide est désactivée. Vous pouvez réactiver la fonction de restauration d'instantané rapide lorsque vous le souhaitez.

Vous pouvez consulter l'état de restauration rapide d'un instantané pour un instantané qui vous appartient ou pour un instantané partagé avec vous.

Console

Pour afficher l'état de la restauration rapide des instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané.
4. Sous l'onglet Details (Détails), Fast Snapshot Restore (Restauration d'instantané rapide) indique l'état de la restauration d'instantané rapide.

AWS CLI

Pour afficher des instantanés avec la restauration rapide des instantanés activée

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-fast-snapshot-restores.html> `describe-fast-snapshot-restore`.

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

Voici un exemple de sortie.

```
{
  "FastSnapshotRestores": [
    {
      "SnapshotId": "snap-0e946653493cb0447",
      "AvailabilityZone": "us-east-2a",
      "State": "enabled",
      "StateTransitionReason": "Client.UserInitiated - Lifecycle state transition",
      "OwnerId": "123456789012",
      "EnablingTime": "2020-01-25T23:57:49.596Z",
      "OptimizingTime": "2020-01-25T23:58:25.573Z",
      "EnabledTime": "2020-01-25T23:59:29.852Z"
    },
    {
      "SnapshotId": "snap-0e946653493cb0447",
      "AvailabilityZone": "us-east-2b",
      "State": "enabled",
      "StateTransitionReason": "Client.UserInitiated - Lifecycle state transition",

```

```

        "OwnerId": "123456789012",
        "EnablingTime": "2020-01-25T23:57:49.596Z",
        "OptimizingTime": "2020-01-25T23:58:25.573Z",
        "EnabledTime": "2020-01-25T23:59:29.852Z"
      }
    ]
  }
}

```

PowerShell

Pour afficher des instantanés avec la restauration rapide des instantanés activée

Utilisez l'applet de commande [Get-EC2FastSnapshotRestore](#).

```

Get-EC2FastSnapshotRestore `
  -Filter @{"Name"="state"; Values="enabled"}

```

Afficher les volumes Amazon EBS restaurés à l'aide de la restauration rapide des instantanés

Lorsque vous créez un volume à partir d'un instantané qui est activé pour la restauration d'instantané rapide dans la zone de disponibilité du volume, il est restauré à l'aide de la restauration d'instantané rapide.

AWS CLI

Pour afficher les volumes créés à partir d'un instantané activé pour la restauration rapide des instantanés

Utilisez la commande [describe-volumes](#).

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

Voici un exemple de sortie.

```

{
  "Volumes": [
    {
      "Attachments": [],
      "AvailabilityZone": "us-east-2a",

```

```
{
  "CreateTime": "2020-01-26T00:34:11.093Z",
  "Encrypted": true,
  "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-a87a-5513e232e843",
  "Size": 20,
  "SnapshotId": "snap-0abcdef1234567890",
  "State": "available",
  "VolumeId": "vol-01234567890abcdef",
  "Iops": 100,
  "VolumeType": "gp2",
  "FastRestored": true
}
```

PowerShell

Pour afficher les volumes créés à partir d'un instantané activé pour la restauration rapide des instantanés

Utilisez l'applet de commande [Get-EC2Volume](#).

```
Get-EC2Volume -Filter @{"Name"="fast-restored"; Values="true"}
```

Verrouillage d'instantanés Amazon EBS

Vous pouvez verrouiller vos instantanés Amazon EBS pour les protéger contre les suppressions accidentelles ou malveillantes, ou pour les stocker au format WORM (write-once-read-many) pendant une durée déterminée. Lorsqu'un instantané est verrouillé, aucun utilisateur ne peut le supprimer, quelles que soient ses autorisations IAM. Une fois qu'il est restauré, vous pouvez utiliser un instantané de la même manière que n'importe quel autre instantané.

Note

Le verrouillage d'instantané a été évalué par Cohasset Associates en vue de son utilisation dans les environnements soumis aux réglementations SEC 17a-4, CFTC et FINRA. Pour de plus amples informations sur la conformité de la fonctionnalité de verrouillage d'instantané vis-à-vis de ces réglementations, consultez le document [Cohasset Associates Compliance Assessment](#).

Vous pouvez verrouiller les instantanés selon le mode de conformité ou le mode de gouvernance, et ils peuvent être verrouillés pendant une durée spécifique ou jusqu'à une date précise. Pour plus d'informations, consultez [Mode de verrouillage](#) et [Durée du verrouillage](#).

Tarification

Vous pouvez verrouiller et déverrouiller les instantanés sans frais supplémentaires. Vous payez les frais de stockage standard des instantanés Amazon EBS pour les instantanés verrouillés.

Rubriques

- [Concepts de verrouillage instantané Amazon EBS](#)
- [Considérations relatives au verrouillage des instantanés Amazon EBS](#)
- [Contrôlez l'accès à Amazon EBS Snapshot Lock](#)
- [Verrouiller un instantané Amazon EBS](#)
- [Débloquez un instantané Amazon EBS](#)
- [Mettre à jour les paramètres de verrouillage des instantanés Amazon EBS](#)
- [Surveiller le verrouillage instantané d'Amazon EBS](#)

Concepts de verrouillage instantané Amazon EBS

Les concepts suivants sont importants à comprendre lorsque vous commencez à utiliser Snapshot Lock.

Table des matières

- [Mode de verrouillage](#)
- [Durée du verrouillage](#)
- [Cooling-off période](#)
- [État du verrouillage](#)

Mode de verrouillage

Vous pouvez verrouiller un instantané dans l'un des deux modes suivants :

Mode gouvernance

Une fois qu'un instantané est verrouillé, les utilisateurs disposant des autorisations IAM appropriées peuvent le déverrouiller et modifier le mode de verrouillage ainsi que la durée ou la date d'expiration du verrouillage à tout moment. Lorsque vous verrouillez un instantané en mode de gouvernance, celui-ci est immédiatement verrouillé ; il n'y a pas de période de réflexion. Pour supprimer un instantané une fois qu'il a été verrouillé en mode de gouvernance, vous devez d'abord le déverrouiller ou attendre que le verrouillage expire.

Vous pouvez utiliser le mode de gouvernance pour répondre aux exigences de gouvernance des données de votre entreprise en vous assurant que seuls certains utilisateurs sont autorisés à déverrouiller des instantanés et à modifier les configurations de verrouillage d'instantané. Vous pouvez également utiliser le mode de gouvernance pour tester la configuration de votre verrouillage avant de verrouiller un instantané en mode de conformité.

Mode conformité

Lorsque vous verrouillez un instantané en mode de conformité, vous pouvez spécifier une période de réflexion qui démarre immédiatement après avoir verrouillé l'instantané. Pendant la période de réflexion, les utilisateurs disposant des autorisations appropriées peuvent déverrouiller l'instantané, modifier le mode de verrouillage, augmenter ou diminuer la période de réflexion et augmenter ou diminuer la durée ou la date d'expiration du verrouillage. Une fois la période de réflexion expirée, vous ne pouvez pas déverrouiller l'instantané, modifier le mode de verrouillage ou réduire la durée ou la date d'expiration du verrouillage ; vous pouvez uniquement augmenter la durée ou la date d'expiration du verrouillage. Pour supprimer un instantané une fois qu'il a été verrouillé conformément à la réglementation et que la période de réflexion a expiré, vous devez attendre que le verrouillage expire.

Note

Vous pouvez verrouiller un instantané en mode de conformité sans période de réflexion en omettant ce délai dans la requête. Dans ce cas, le verrouillage devient effectif immédiatement, et vous ne pouvez pas déverrouiller l'instantané, modifier le mode de verrouillage ou réduire la durée ou la date d'expiration du verrouillage ; vous pouvez uniquement augmenter la durée ou la date d'expiration du verrouillage.

Vous pouvez utiliser le mode de conformité pour protéger les instantanés qui ne doivent pas être supprimés pendant une période spécifique pour des raisons de conformité. Le mode de conformité offre les avantages suivants :

- il permet la configuration WORM (write-once, read-many) pour vos instantanés ;
- il fournit une couche de défense supplémentaire qui protège les instantanés contre les suppressions accidentelles ou malveillantes ;
- il applique des périodes de conservation, qui empêchent les suppressions anticipées par des utilisateurs privilégiés, afin de respecter les politiques et procédures de protection des données de votre entreprise.

Note

La seule façon de supprimer un instantané verrouillé en mode de conformité avant l'expiration de son verrouillage est de fermer le AWS compte associé.

Durée du verrouillage

La durée du verrouillage est la période pendant laquelle l'instantané doit rester verrouillé. Vous pouvez spécifier la durée du verrouillage d'une des deux façons suivantes, mais des deux en même temps :

Nombre de jours

La durée du verrouillage est spécifiée sous la forme d'un nombre de jours pendant lesquels l'instantané doit rester verrouillé. Une fois le nombre de jours spécifié écoulé, l'instantané est automatiquement déverrouillé. La durée peut aller de 1 jour à 36 500 jours (100 ans).

Date d'expiration du verrouillage

La durée du verrouillage est déterminée par une date d'expiration future. L'instantané reste verrouillé jusqu'à ce que la date d'expiration du verrouillage soit atteinte. Lorsque la date d'expiration du verrouillage est atteinte, l'instantané est automatiquement déverrouillé.

Cooling-off période

La période de réflexion est une période facultative que vous pouvez spécifier lorsque vous verrouillez un instantané en mode de conformité. Pendant la période de réflexion, les utilisateurs disposant des autorisations appropriées peuvent déverrouiller l'instantané, modifier le mode de verrouillage, augmenter ou diminuer la période de réflexion et augmenter ou diminuer la durée du verrouillage. Une fois la période de réflexion expirée, les utilisateurs ne peuvent pas déverrouiller l'instantané,

modifier le mode de verrouillage, rétablir la période de réflexion ou réduire la durée du verrouillage, quelles que soient leurs autorisations.

Il n'est pas possible de supprimer un instantané pendant la période de réflexion.

Si cela est spécifié, la période de réflexion commence immédiatement après le verrouillage de l'instantané. Si cela est omis, l'instantané est immédiatement verrouillé en mode de conformité sans période de réflexion.

La période de réflexion peut aller de 1 à 72 heures. Pour verrouiller un instantané en mode de conformité immédiatement sans période de réflexion, ne spécifiez pas ce délai dans la requête.

État du verrouillage

Un verrouillage d'instantané peut avoir l'un des états suivants :

- **compliance-cooloff** : l'instantané a été verrouillé en mode de conformité, mais sa période de réflexion est toujours en cours. L'instantané ne peut pas être supprimé, mais il peut être déverrouillé et les paramètres de verrouillage peuvent être modifiés par les utilisateurs disposant des autorisations appropriées.
- **governance** : l'instantané est verrouillé en mode de gouvernance. L'instantané ne peut pas être supprimé, mais il peut être déverrouillé et les paramètres de verrouillage peuvent être modifiés par les utilisateurs disposant des autorisations appropriées.
- **compliance** : l'instantané est verrouillé en mode de conformité sans période de réflexion ou la période de réflexion a expiré. L'instantané ne peut pas être déverrouillé ou supprimé. La durée du verrouillage ne peut être augmentée que par les utilisateurs disposant des autorisations appropriées.
- **expired** : l'instantané a été verrouillé en mode de conformité ou de gouvernance, mais le verrouillage a expiré. L'instantané n'est pas verrouillé et peut être supprimé.

Considérations relatives au verrouillage des instantanés Amazon EBS

Gardez les points suivants à l'esprit lorsque vous verrouillez des instantanés Amazon EBS.

- Vous ne pouvez verrouiller un instantané que s'il est à l'état `pending` ou `completed`.
 - Si vous verrouillez un instantané alors qu'il est à l'état `pending`, et que vous le verrouillez pendant une durée spécifique, la durée de verrouillage ne commence que lorsque l'instantané atteint l'état `completed`. L'instantané ne peut pas être supprimé tant qu'il est à l'état `pending`.

- Si vous verrouillez un instantané alors qu'il est à l'état `pending` et que la création de l'instantané échoue pour une raison quelconque, le verrouillage est annulé.
- Si vous prolongez la durée de verrouillage d'un instantané verrouillé en mode de conformité après l'expiration de la période de réflexion, vous ne pouvez pas spécifier une autre période de réflexion. Si vous spécifiez une période de réflexion, la requête échoue.
- Vous pouvez verrouiller les instantanés archivés. Et vous pouvez archiver les instantanés verrouillés.
- Vous pouvez verrouiller les instantanés associés à une AMI.
- Vous pouvez annuler l'inscription d'une AMI qui a des instantanés verrouillés associés.
- Vous pouvez supprimer la clé KMS utilisée pour chiffrer un instantané verrouillé.
- Nous vous recommandons de ne pas verrouiller les instantanés créés par AWS Backup. AWS Backup garantit déjà que ses instantanés ne sont pas supprimés avant l'expiration de leur période de conservation. Pour ajouter une couche de sécurité supplémentaire aux instantanés gérés par AWS Backup, nous vous recommandons d'utiliser AWS Backup Vault Lock. Pour plus d'informations, consultez la page [AWS Backup Vault Lock](#).
- Vous ne pouvez pas verrouiller les instantanés lors de leur création ou de l'inscription de l'AMI.
- Vous ne pouvez pas verrouiller les instantanés Amazon EBS locaux sur AWS Outposts.
- La seule façon de supprimer un instantané verrouillé en mode de conformité avant l'expiration de son verrouillage est de fermer le AWS compte associé.

Si vous fermez votre AWS compte alors que vous avez verrouillé les instantanés, il AWS est suspendu pendant 90 jours avec vos instantanés intacts. Si vous ne rouvrez pas votre compte dans les 90 jours, vos instantanés AWS seront supprimés, même s'ils sont verrouillés.

Contrôlez l'accès à Amazon EBS Snapshot Lock

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les verrouillages d'instantanés. Pour permettre aux utilisateurs d'utiliser les verrouillages d'instantanés, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Pour plus d'informations, consultez [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Rubriques

- [Autorisations requises](#)
- [Limitation de l'accès avec des clés de condition](#)

Autorisations requises

Pour utiliser les verrouillages d'instantanés, les utilisateurs ont besoin des autorisations suivantes.

- `ec2:LockSnapshot` : pour verrouiller les instantanés.
- `ec2:UnlockSnapshot` : pour déverrouiller les instantanés.
- `ec2:DescribeLockedSnapshots` : pour afficher les paramètres de verrouillage d'instantané.

Voici un exemple de politique IAM qui autorise les utilisateurs à verrouiller et déverrouiller des instantanés et à afficher les paramètres de verrouillage d'instantané. Elle inclut l'autorisation `ec2:DescribeSnapshots` pour les utilisateurs de la console. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSnapshotLockOperations",
      "Effect": "Allow",
      "Action": [
        "ec2:LockSnapshot",
        "ec2:UnlockSnapshot",
        "ec2:DescribeLockedSnapshots",
        "ec2:DescribeSnapshots"
      ],
      "Resource": [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:111122223333:volume/*"
      ]
    }
  ]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Limitation de l'accès avec des clés de condition

Vous pouvez utiliser des clés de condition pour limiter la manière dont les utilisateurs sont autorisés à verrouiller les instantanés.

Rubriques

- [EC2 : SnapshotLockDuration](#)
- [EC2 : CoolOffPeriod](#)

EC2 : SnapshotLockDuration

Vous pouvez utiliser la clé de condition `ec2:SnapshotLockDuration` pour limiter les utilisateurs à des durées de verrouillage spécifiques lors du verrouillage d'instantanés.

L'exemple de politique suivant limite les utilisateurs à spécifier une durée de verrouillage comprise entre 10 et 50 jours.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowSnapshotLockWithDurationCondition",
    "Effect": "Allow",
    "Action": "ec2:LockSnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:SnapshotLockDuration": 10
      },
      "NumericLessThan": {
        "ec2:SnapshotLockDuration": 50
      }
    }
  }
]
}

```

EC2 : CoolOffPeriod

Vous pouvez utiliser la clé de condition `ec2:CoolOffPeriod` pour empêcher les utilisateurs de verrouiller les instantanés en mode de conformité sans période de réflexion.

L'exemple de politique suivant limite les utilisateurs à spécifier une période de réflexion supérieure à 48 heures lorsqu'ils verrouillent des instantanés en mode de conformité.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSnapshotLockWithCondition",
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "NumericGreaterThan": {
          "ec2:SnapshotTime": 48
        }
      }
    }
  ]
}

```

```
}  
}  
}  
]  
}
```

Verrouiller un instantané Amazon EBS

Vous pouvez verrouiller un instantané qui est à l'état pending ou completed. Pour de plus amples informations, veuillez consulter [Considérations relatives au verrouillage des instantanés Amazon EBS](#).

Console

Pour verrouiller un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Sélectionnez l'instantané à verrouiller, puis choisissez Actions, Paramètres d'instantané, Gérer le verrouillage d'instantané.
4. Sélectionnez Verrouiller l'instantané.
5. Pour Mode de verrouillage, choisissez Mode de gouvernance ou Mode de conformité. Pour de plus amples informations, veuillez consulter [Mode de verrouillage](#).
6. Pour Durée du verrouillage, effectuez l'une des opérations suivantes :
 - Pour verrouiller l'instantané pendant une période spécifique, choisissez Verrouiller l'instantané pour, puis saisissez la période en jours ou en années.
 - Pour verrouiller l'instantané jusqu'à une date et une heure spécifiques, choisissez Verrouiller l'instantané jusqu'à, puis sélectionnez la date et l'heure d'expiration.

Pour de plus amples informations, veuillez consulter [Durée du verrouillage](#).

7. (Mode conformité uniquement) Pour ce qui est de la Cooling-off période, spécifiez une période de réflexion pendant laquelle vous pouvez déverrouiller l'instantané et modifier la configuration du verrouillage. Pour de plus amples informations, veuillez consulter [Cooling-off période](#).

8. (Mode de conformité uniquement) Pour confirmer que vous souhaitez verrouiller l'instantané en mode de conformité et que vous ne pourrez pas le déverrouiller après l'expiration de la période de réflexion, choisissez Reconnaître.
9. Choisissez Enregistrer les paramètres de verrouillage.

AWS CLI

Pour verrouiller un instantané en mode de gouvernance

Utilisez la commande [lock-snapshot](#). Pour `--lock-mode`, spécifiez `governance`. Pour verrouiller l'instantané pendant une période spécifique, pour `--lock-duration`, spécifiez la période, en jours.

```
aws ec2 lock-snapshot \  
  --snapshot-id snap-0abcdef1234567890 \  
  --lock-mode governance \  
  --lock-duration 30
```

Pour verrouiller l'instantané jusqu'à une date précise, pour `--expiration-date`, spécifiez la date et l'heure auxquelles le verrouillage doit expirer, dans le fuseau horaire UTC.

```
aws ec2 lock-snapshot \  
  --snapshot-id snap-0abcdef1234567890 \  
  --lock-mode governance \  
  --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Pour verrouiller un instantané en mode de conformité

Utilisez la commande [lock-snapshot](#). Pour `--lock-mode`, spécifiez `compliance`. Pour `--cool-off-period`, spécifiez éventuellement une période de refroidissement, en heures. Pour verrouiller l'instantané pendant une période spécifique, pour `--lock-duration`, spécifiez le nombre de jours pendant lequel le cliché doit être verrouillé.

```
aws ec2 lock-snapshot \  
  --snapshot-id snap-0abcdef1234567890 \  
  --lock-mode compliance \  
  --cool-off-period 24 \  
  --lock-duration 30
```

Pour verrouiller l'instantané jusqu'à une date précise, pour `--expiration-date`, spécifiez la date et l'heure auxquelles le verrouillage doit expirer, dans le fuseau horaire UTC.

```
aws ec2 lock-snapshot \  
  --snapshot-id snap-0abcdef1234567890 \  
  --lock-mode compliance \  
  --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

PowerShell

Pour verrouiller un instantané en mode de gouvernance

Utilisez l'applet de commande [Lock-EC2Snapshot](#). Vous pouvez éventuellement spécifier la durée du verrouillage du snapshot, en jours.

```
Lock-EC2Snapshot `\  
  -SnapshotId snap-0abcdef1234567890 `\  
  -LockMode "governance" `\  
  -LockDuration 30
```

Vous pouvez également verrouiller l'instantané jusqu'à une date précise, dans le fuseau horaire UTC.

```
Lock-EC2Snapshot `\  
  -SnapshotId snap-0abcdef1234567890 `\  
  -LockMode "governance" `\  
  -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

Pour verrouiller un instantané en mode de conformité

Utilisez l'applet de commande [Lock-EC2Snapshot](#). Vous pouvez éventuellement spécifier une période de réflexion, en heures. Vous pouvez également éventuellement spécifier la durée du verrouillage du snapshot, en jours.

```
Lock-EC2Snapshot `\  
  -SnapshotId snap-0abcdef1234567890 `\  
  -LockMode "compliance" `\  
  -CooloffPeriod 24 `\  
  -LockDuration 30
```

Vous pouvez également verrouiller l'instantané jusqu'à une date précise, dans le fuseau horaire UTC.

```
Lock-EC2Snapshot `
  -SnapshotId snap-0abcdef1234567890 `
  -LockMode "compliance" `
  -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

Débloquez un instantané Amazon EBS

Vous ne pouvez déverrouiller un instantané que s'il est verrouillé en mode de gouvernance ou s'il est verrouillé en mode de conformité et qu'il est toujours dans la période de réflexion.

Console

Pour déverrouiller un instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Sélectionnez l'instantané à déverrouiller, puis choisissez Actions, Paramètres d'instantané, Gérer le verrouillage d'instantané.
4. Choisissez Déverrouiller un instantané, puis choisissez à nouveau Déverrouiller un instantané pour confirmer.

AWS CLI

Pour déverrouiller un instantané

Utilisez la commande [unlock-snapshot](#).

```
aws ec2 unlock-snapshot --snapshot-id snap-0abcdef1234567890
```

PowerShell

Pour déverrouiller un instantané

Utilisez l'applet de commande [Unlock-EC2Snapshot](#).


```
Unlock-EC2Snapshot --SnapshotId snap-0abcdef1234567890
```

Mettre à jour les paramètres de verrouillage des instantanés Amazon EBS

Les mises à jour autorisées dépendent de l'état du verrouillage :

- **governance** : vous pouvez modifier le mode de verrouillage et augmenter ou diminuer la durée ou la date d'expiration du verrouillage.
- **compliance-cooloff** : vous pouvez modifier le mode de verrouillage, augmenter ou diminuer la période de réflexion, et augmenter ou diminuer la durée ou la date d'expiration du verrouillage.
- **compliance** : vous pouvez uniquement augmenter la durée ou la date d'expiration du verrouillage.

Console

Pour mettre à jour les paramètres de verrouillage d'instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés).
3. Sélectionnez l'instantané pour lequel vous souhaitez modifier les paramètres de verrouillage, puis choisissez Actions, Paramètres d'instantané, Gérer le verrouillage d'instantané.
4. Mettez à jour les paramètres selon vos besoins, puis choisissez Enregistrer les paramètres de verrouillage.

AWS CLI

Pour mettre à jour les paramètres de verrouillage d'instantané

Utilisez la commande [lock-snapshot](#). Spécifiez l'ID de l'instantané et les options à modifier. L'exemple suivant modifie la date d'expiration.

```
aws ec2 lock-snapshot \  
  --snapshot-id snap-0abcdef1234567890 \  
  --lock-mode governance \  
  --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

PowerShell

Pour mettre à jour les paramètres de verrouillage d'instantané

Utilisez l'applet de commande [Lock-EC2Snapshot](#). Spécifiez l'ID de l'instantané et les options à modifier. L'exemple suivant modifie la date d'expiration.

```
Lock-EC2Snapshot `
  -SnapshotId snap-0abcdef1234567890 `
  -LockMode "governance" `
  -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

Surveiller le verrouillage instantané d'Amazon EBS

Vous pouvez surveiller les actions liées au verrouillage des instantanés Amazon EBS à l'aide des outils suivants :

Rubriques

- [Surveillez les blocages des snapshots Amazon EBS à l'aide de AWS CloudTrail](#)
- [Surveillez les blocages des snapshots Amazon EBS à l'aide d'Amazon EventBridge](#)

Surveillez les blocages des snapshots Amazon EBS à l'aide de AWS CloudTrail

Vous pouvez surveiller les appels d'API pour les blocages de snapshots en tant qu'événements, y compris les appels depuis la console et les appels de code vers les API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite, 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 plus d'informations, consultez [Consigner les appels d'API à l'aide de AWS CloudTrail](#).

Surveillez les blocages des snapshots Amazon EBS à l'aide d'Amazon EventBridge

Amazon EBS émet des événements liés aux actions de verrouillage d'instantané. Vous pouvez utiliser AWS Lambda Amazon EventBridge pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur [Amazon](#).

Les événements suivants sont émis :

- Instantané verrouillé avec succès en mode de gouvernance ou de conformité.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "source": 012345678901,
    "lockState": "compliance-cooloff",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "coolOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Échec du verrouillage lorsqu'un instantané est verrouillé alors qu'il est à l'état pending et qu'il ne parvient pas à atteindre l'état completed.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
```

```

    "event": "lockSnapshot",
    "result": "failed",
    "cause": "snapshot failed",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "pending-compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "coolOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}

```

- Verrouillage expiré

```

{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockDurationExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "expired",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123
  }
}

```

- Cooling-off la période a expiré après avoir été verrouillé en mode conformité.

```

{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",

```

```
"source": "aws.ec2",
"account": "012345678901",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "us-east-1",
"resources": [
  "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
],
"detail": {
  "event": "cooloffperiodExpiry",
  "result": "succeeded",
  "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
  "lockState": "compliance",
  "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
  "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
  "lockDuration": 123,
  "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
  "coolOffPeriod": 24,
  "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
}
```

Bloquer l'accès public aux instantanés Amazon EBS

Pour empêcher le partage public de vos instantanés, vous pouvez activer le blocage de l'accès public pour les instantanés. Une fois que vous avez activé le blocage de l'accès public pour les instantanés dans une région, toute tentative de partage public d'instantanés dans cette région est automatiquement bloquée. Cela peut vous aider à améliorer la sécurité de vos instantanés et à protéger les données de vos instantanés contre tout accès non autorisé ou involontaire.

Le blocage de l'accès public pour les instantanés peut être activé dans l'un des deux modes suivants :

- Bloquer tous les partages : bloque tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- Bloquer les nouveaux partages : bloque tout nouveau partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

Considérations

Gardez les points suivants à l'esprit lorsque vous utilisez le blocage de l'accès public pour les instantanés.

- Bloquer l'accès public aux instantanés n'empêche pas le partage d'instantanés privés.
- L'activation du blocage de l'accès public aux instantanés en mode Bloquer tout partage ne modifie pas les autorisations pour les instantanés déjà partagés publiquement. À la place, ces instantanés ne sont plus visibles et accessibles au public. Les attributs de ces instantanés indiquent donc toujours qu'ils sont partagés publiquement, même s'ils ne sont pas accessibles au public.

Si vous désactivez ultérieurement le blocage de l'accès public ou si vous modifiez le mode pour bloquer un nouveau partage, ces instantanés seront à nouveau accessibles au public.

- Le blocage de l'accès public pour les instantanés est un paramètre régional. Il s'applique à tous les instantanés de la région dans laquelle il est activé. Vous devez activer le blocage de l'accès public pour les instantanés dans chaque région dans laquelle vous souhaitez empêcher le partage public de vos instantanés.
- Le bloquer de l'accès public est un paramètre défini au niveau du compte. Il s'applique à tous les utilisateurs du compte, y compris aux utilisateurs administrateurs. Vous ne pouvez pas activer le blocage de l'accès public pour les instantanés au niveau de l'entreprise.
- Le paramètre de blocage de l'accès public est configuré soit directement dans le compte, soit à l'aide d'une politique déclarative. L'utilisation d'une politique déclarative vous permet d'appliquer le paramètre à plusieurs régions simultanément, ainsi qu'à plusieurs comptes simultanément. Lorsqu'une politique déclarative est utilisée, vous ne pouvez pas modifier le paramètre directement dans un compte. Cette rubrique décrit comment configurer le paramètre directement dans un compte. Pour plus d'informations sur l'utilisation des politiques déclaratives, consultez la section [Politiques déclaratives](#) dans le Guide de l'utilisateur AWS Organizations .
- Bloquer l'accès public aux instantanés n'empêche pas le partage public des EBS-backed AMI. Si vous activez le blocage de l'accès public pour les instantanés, les utilisateurs peuvent toujours partager publiquement des EBS-backed AMI. Si une EBS-backed AMI est partagée publiquement, les utilisateurs ayant accès à cette AMI peuvent créer des volumes à partir de ses instantanés associés. Pour empêcher le partage public de vos AMI, activez l'option [Bloquer l'accès public aux AMI](#) .
- Le blocage de l'accès public aux instantanés n'est pas pris en charge lorsque les instantanés locaux sont activés. AWS Outposts

Tarification

Le blocage de l'accès public pour les instantanés peut être activé sans frais supplémentaires.

Table des matières

- [Autorisations IAM pour bloquer l'accès public aux instantanés Amazon EBS](#)
- [Configurer l'accès public par blocage pour les instantanés Amazon EBS](#)
- [Afficher le paramètre de blocage de l'accès public pour les instantanés Amazon EBS](#)
- [Désactiver le blocage de l'accès public pour les instantanés Amazon EBS](#)
- [Surveillez et bloquez l'accès public aux instantanés Amazon EBS à l'aide de EventBridge](#)

Autorisations IAM pour bloquer l'accès public aux instantanés Amazon EBS

Par défaut, les utilisateurs ne sont pas autorisés à utiliser le blocage de l'accès public pour les instantanés. Pour permettre aux utilisateurs d'utiliser le blocage de l'accès public pour les instantanés, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter les autorisations à vos utilisateurs, groupes ou rôles.

Pour utiliser le blocage de l'accès public pour les instantanés, les utilisateurs ont besoin des autorisations suivantes.

- `ec2:EnableSnapshotBlockPublicAccess` : activer le blocage de l'accès public pour les instantanés et modifier le mode.
- `ec2:DisableSnapshotBlockPublicAccess` : désactiver le blocage de l'accès public pour les instantanés
- `ec2:GetSnapshotBlockPublicAccessState` : afficher le paramètre de blocage de l'accès public pour instantanés pour une région.

Voici un exemple de politique IAM. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

JSON

```
{  
  "Version": "2012-10-17",
```

```

    "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:EnableSnapshotBlockPublicAccess",
        "ec2:DisableSnapshotBlockPublicAccess",
        "ec2:GetSnapshotBlockPublicAccessState"
      ],
      "Resource": "*"
    }]
  }

```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :
 - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
 - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Configurer l'accès public par blocage pour les instantanés Amazon EBS

Activez le blocage de l'accès public pour les instantanés pour empêcher le partage public des instantanés dans la région. Une fois cette fonctionnalité activée, les demandes de partage public d'instantanés dans la région sont bloquées.

Important

L'activation du blocage de l'accès public aux instantanés en mode Bloquer tout partage ne modifie pas les autorisations pour les instantanés déjà partagés publiquement. À la

place, ces instantanés ne sont plus visibles et accessibles au public. Les attributs de ces instantanés indiquent donc toujours qu'ils sont partagés publiquement, même s'ils ne sont pas accessibles au public.

Si vous désactivez ultérieurement le blocage de l'accès public ou si vous modifiez le mode pour bloquer un nouveau partage, ces instantanés seront à nouveau accessibles au public.

Note

Ce paramètre est configuré au niveau du compte, soit directement dans le compte, soit à l'aide d'une politique déclarative. Il doit être configuré dans chaque Région AWS endroit où vous souhaitez empêcher le partage public des instantanés. L'utilisation d'une politique déclarative vous permet d'appliquer le paramètre à plusieurs régions simultanément, ainsi qu'à plusieurs comptes simultanément. Lorsqu'une politique déclarative est utilisée, vous ne pouvez pas modifier le paramètre directement dans un compte. Cette rubrique décrit comment configurer le paramètre directement dans un compte. Pour plus d'informations sur l'utilisation des politiques déclaratives, consultez la section [Politiques déclaratives](#) dans le Guide de l'utilisateur AWS Organizations .

Console

Pour configurer le blocage de l'accès public pour les instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Tableau de bord EC2, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. Dans la section Bloquer l'accès public pour les instantanés EBS, choisissez Gérer.
4. Sélectionnez Bloquer l'accès public, puis choisissez l'une des options suivantes :
 - Bloquer tous les accès publics : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
 - Bloquer les nouveaux partages publics : pour bloquer tout nouveau partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage

public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

5. Choisissez Mettre à jour.

AWS CLI

Pour activer ou modifier le blocage de l'accès public pour les instantanés

Utilisez la commande [enable-snapshot-block-public-access](#). Pour `--state`, spécifiez l'une des valeurs suivantes :

- `block-all-sharing` : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- `block-new-sharing` : pour bloquer uniquement les nouveaux partages publics de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

Pour activer ou modifier, bloquer l'accès public aux instantanés d'une région spécifique

```
aws ec2 enable-snapshot-block-public-access \
  --state block-new-sharing \
  --region us-east-1
```

Voici un exemple de sortie.

```
{
  "State": "block-new-sharing"
}
```

Pour activer ou modifier, bloquer l'accès public aux instantanés pour toutes les régions

```
echo -e "Region \t Public Access State" ; \
echo -e "----- \t -----" ; \
for region in $(
  aws ec2 describe-regions \
    --region us-east-1 \
    --query "Regions[*].[RegionName]" \
    --output text
```

```

);
do (output=$(
    aws ec2 enable-snapshot-block-public-access \
        --region $region \
        --state block-new-sharing \
        --output text)
    echo -e "$region \t $output"
);
done

```

Voici un exemple de sortie.

Region	Public Access State
-----	-----
ap-south-1	block-new-sharing
eu-north-1	block-new-sharing
eu-west-3	block-new-sharing
...	

PowerShell

Pour activer ou modifier le blocage de l'accès public pour les instantanés

Utilisez la commande [Enable-EC2SnapshotBlockPublicAccess](#). Pour -State, spécifiez l'une des valeurs suivantes :

- `block-all-sharing` : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- `block-new-sharing` : pour bloquer uniquement les nouveaux partages publics de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

Pour activer ou modifier, bloquer l'accès public aux instantanés d'une région spécifique

```

Enable-EC2SnapshotBlockPublicAccess `
    -Region us-east-1 `
    -State block-new-sharing

```

Voici un exemple de sortie.

```
Value
-----
block-new-sharing
```

Pour activer ou modifier, bloquer l'accès public aux instantanés pour toutes les régions

```
(Get-EC2Region -Region us-east-1).RegionName | `
  ForEach-Object {
    [PSCustomObject]@{
      Region          = $_
      PublicAccessState = (
        Enable-EC2SnapshotBlockPublicAccess `
          -Region $_ `
          -State block-new-sharing)
    }
  } | Format-Table -AutoSize
```

Voici un exemple de sortie.

```
Region          PublicAccessState
-----
ap-south-1      block-new-sharing
eu-north-1      block-new-sharing
eu-west-3       block-new-sharing
...
```

Afficher le paramètre de blocage de l'accès public pour les instantanés Amazon EBS

Vous pouvez bloquer l'accès public dans l'un des états suivants pour chaque région de votre compte.

- **Bloquer tous les partages** : tous les partages publics de vos instantanés sont bloqués. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont pas accessibles au public.
- **Bloquer les nouveaux partages** : seuls les nouveaux partages de vos instantanés sont bloqués. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

- Débloqué : le partage public n'est pas bloqué. Les utilisateurs peuvent partager des instantanés publiquement.

Console

Pour afficher le paramètre de blocage de l'accès public pour les instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Tableau de bord EC2, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. La section Bloquer l'accès public pour les instantanés EBS montre le paramètre actuel.

AWS CLI

Pour afficher le paramètre de blocage de l'accès public pour les instantanés

Utilisez la commande [get-snapshot-block-public-access-state](#).

- Pour une région spécifique

```
aws ec2 get-snapshot-block-public-access-state
```

Dans cet exemple de sortie, le ManagedBy champ indique l'entité qui a configuré le paramètre et account indique que le paramètre a été configuré directement dans le compte. Une valeur de declarative-policy signifierait que le paramètre a été configuré par une politique déclarative. Pour plus d'informations, consultez la rubrique [Politiques déclaratives](#) dans le Guide de l'utilisateur AWS Organizations .

```
{
  "State": "unblocked",
  "ManagedBy": "account"
}
```

- Pour toutes les régions

```
echo -e "Region \t Public Access State" ; \
echo -e "----- \t -----" ; \
for region in $(
  aws ec2 describe-regions \
```

```

    --region us-east-1 \
    --query "Regions[*].[RegionName]" \
    --output text
);
do (output=$(
    aws ec2 get-snapshot-block-public-access-state \
        --region $region \
        --output text)
    echo -e "$region \t $output"
);
done

```

Voici un exemple de sortie.

Region	Public Access State
-----	-----
ap-south-1	unblocked
eu-north-1	unblocked
eu-west-3	unblocked

PowerShell

Pour afficher le paramètre de blocage de l'accès public pour les instantanés

Utilisez l' [Get-EC2SnapshotBlockPublicAccessState](#) applet de commande.

- Pour une région spécifique

```
Get-EC2SnapshotBlockPublicAccessState -Region us-east-1
```

Voici un exemple de sortie.

```

Value
-----
block-new-sharing

```

- Pour toutes les régions

```

(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
        [PSCustomObject]@{

```

```

        Region          = $_
        PublicAccessState = (Get-EC2SnapshotBlockPublicAccessState -Region $_)
    }
} | Format-Table -AutoSize

```

Voici un exemple de sortie.

Region	Public Access State
-----	-----
ap-south-1	unblocked
eu-north-1	unblocked
eu-west-3	unblocked
...	

Désactiver le blocage de l'accès public pour les instantanés Amazon EBS

Désactivez le blocage de l'accès public pour les instantanés pour autoriser le partage public des instantanés dans la région. Une fois cette fonctionnalité désactivée, les utilisateurs peuvent partager publiquement des instantanés dans la région.

Important

L'activation du blocage de l'accès public aux instantanés en mode Bloquer tout partage ne modifie pas les autorisations pour les instantanés déjà partagés publiquement. À la place, ces instantanés ne sont plus visibles et accessibles au public. Les attributs de ces instantanés indiquent donc toujours qu'ils sont partagés publiquement, même s'ils ne sont pas accessibles au public.

Si vous désactivez le blocage de l'accès public, ces instantanés seront à nouveau accessibles au public.

Note

Ce paramètre est configuré au niveau du compte, soit directement dans le compte, soit à l'aide d'une politique déclarative. Il doit être configuré dans chaque Région AWS endroit où vous souhaitez autoriser le partage public des instantanés. L'utilisation d'une politique déclarative vous permet d'appliquer le paramètre à plusieurs régions simultanément, ainsi qu'à plusieurs comptes simultanément. Lorsqu'une politique déclarative est utilisée, vous

ne pouvez pas modifier le paramètre directement dans un compte. Cette rubrique décrit comment configurer le paramètre directement dans un compte. Pour plus d'informations sur l'utilisation des politiques déclaratives, consultez la section [Politiques déclaratives](#) dans le Guide de l'utilisateur AWS Organizations .

Console

Pour désactiver le blocage de l'accès public pour les instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Tableau de bord EC2, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. Dans la section Bloquer l'accès public pour les instantanés EBS, choisissez Gérer.
4. Effacez Bloquer l'accès public et choisissez Enregistrer.

AWS CLI

Pour désactiver le blocage de l'accès public pour les instantanés

Utilisez la commande [disable-snapshot-block-public-access](#).

- Pour une région spécifique

```
aws ec2 disable-snapshot-block-public-access --region us-east-1
```

Voici un exemple de sortie.

```
{  
  "State": "unblocked"  
}
```

- Pour toutes les régions

```
echo -e "Region \t Public Access State" ; \  
echo -e "----- \t -----" ; \  
for region in $(  
  aws ec2 describe-regions \  
    --region us-east-1 \  
  )  
do  
  aws ec2 disable-snapshot-block-public-access --region $region  
done
```



```

        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-snapshot-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done

```

Voici un exemple de sortie.

Region	Public Access State
-----	-----
ap-south-1	unblocked
eu-north-1	unblocked
eu-west-3	unblocked

PowerShell

Pour désactiver le blocage de l'accès public pour les instantanés

Utilisez l' [Disable-EC2SnapshotBlockPublicAccess](#) applet de commande.

- Pour une région spécifique

```
Disable-EC2SnapshotBlockPublicAccess -Region us-east-1
```

Voici un exemple de sortie.

```

Value
-----
unblocked

```

- Pour toutes les régions

```

(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
        [PSCustomObject]@{
            Region      = $_

```

```

        PublicAccessState = (Disable-EC2SnapshotBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize

```

Voici un exemple de sortie.

Region	PublicAccessState
-----	-----
ap-south-1	unblocked
eu-north-1	unblocked
eu-west-3	unblocked
...	

Surveillez et bloquez l'accès public aux instantanés Amazon EBS à l'aide de EventBridge

Amazon EBS émet des événements liés au blocage de l'accès public pour les instantanés. Vous pouvez utiliser AWS Lambda Amazon EventBridge pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur [Amazon](#).

Les événements suivants sont émis :

- Activation du blocage de l'accès public pour les instantanés en mode bloquer tous les partages

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-all-sharing",
    "message": "Block Public Access was successfully enabled in 'block-all-sharing' mode"
  }
}

```

- Activation du blocage de l'accès public pour les instantanés en mode bloquer les nouveaux partages

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-new-sharing",
    "message": "Block Public Access was successfully enabled in 'block-new-sharing' mode"
  }
}
```

- Désactivation du blocage de l'accès public pour les instantanés

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Disabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "unblocked",
    "message": "Block Public Access was successfully disabled"
  }
}
```

Instantanés locaux Amazon EBS sur Outposts

Les instantanés Amazon EBS sont une copie ponctuelle de vos volumes EBS.

Par défaut, les instantanés des volumes EBS sur un AWS Outpost sont stockés dans Amazon S3 dans la région du Outpost. Vous pouvez également utiliser les instantanés locaux d'Amazon EBS sur Outposts pour stocker des instantanés des volumes sur et Outpost localement dans Amazon S3 sur

lui-même. Outpost Cela garantit que les données des instantanés se Outpost trouvent sur et dans vos locaux. En outre, vous pouvez utiliser les politiques et autorisations Gestion des identités et des accès AWS (IAM) pour configurer des politiques d'application de la résidence des données afin de vous assurer que les données des instantanés ne quittent pas le. Outpost Cela est particulièrement utile si vous résidez dans un pays ou une région qui n'est pas encore desservie par une AWS région et qui impose des exigences en matière de résidence des données.

Cette rubrique fournit des informations sur l'utilisation d'Instantanés locaux Amazon EBS sur Outposts. Pour plus d'informations sur les instantanés Amazon EBS et sur l'utilisation des instantanés dans une AWS région, consultez. [Instantanés Amazon EBS](#)

Pour plus d'informations, consultez [AWS Outposts la section Famille](#) et documentation relative à la [AWS Outposts famille](#).

Rubriques

- [Questions fréquentes \(FAQ\)](#)
- [Conditions préalables](#)
- [Considérations](#)
- [Contrôle de l'accès avec IAM](#)
- [Utilisation des instantanés locaux](#)

Questions fréquentes (FAQ)

1. Présentation d'instantanés locaux

Par défaut, les instantanés Amazon EBS des volumes d'un Outpost sont stockés dans Amazon S3 dans la région du. Outpost S'il Outpost est configuré avec S3 sur Outposts, vous pouvez choisir de stocker les instantanés localement sur lui-même. Outpost Les instantanés sont des sauvegardes incrémentielles, ce qui signifie que seuls les blocs du volume qui ont changé depuis votre instantané le plus récent sont enregistrés. Vous pouvez utiliser ces instantanés pour restaurer un volume Outpost identique à l'instantané à tout moment. Pour plus d'informations sur les instantanés Amazon EBS, consultez [Instantanés Amazon EBS](#).

2. Pourquoi utiliser des instantanés locaux ?

Les instantanés constituent un moyen pratique de sauvegarder vos données. Avec les instantanés locaux, toutes les données de vos instantanés sont stockées localement sur le Outpost. Cela signifie qu'il ne quitte pas vos locaux. Cela est particulièrement utile si vous

résidez dans un pays ou une région qui n'est pas encore desservi par une AWS région et qui impose des conditions de résidence.

En outre, l'utilisation d'instantanés locaux peut contribuer à réduire la bande passante utilisée pour les communications entre la région et les environnements Outpost à bande passante limitée.

3. Comment puis-je appliquer la résidence des données des instantanés sur un Outpost ?

Vous pouvez utiliser des politiques Gestion des identités et des accès AWS (IAM) pour contrôler les autorisations dont disposent les principaux utilisateurs (AWS comptes, utilisateurs IAM et rôles IAM) lorsqu'ils travaillent avec des instantanés locaux et pour appliquer la résidence des données. Vous pouvez créer une politique qui empêche les administrateurs de créer des instantanés à partir de Outpost volumes et d'instances et de stocker les instantanés dans une région. AWS Actuellement, la copie d'instantanés et d'images depuis et Outpost vers une région n'est pas prise en charge. Pour plus d'informations, consultez [Contrôle de l'accès avec IAM](#).

4. Les instantanés locaux à volumes multiples et cohérents en cas d'incidents sont-ils pris en charge ?

Oui, vous pouvez créer des instantanés locaux multivolumes et cohérents en cas de crash à partir d'instances sur un Outpost.

5. Comment créer des instantanés locaux ?

Vous pouvez créer des instantanés manuellement à l'aide de la AWS Command Line Interface (AWS CLI) ou de la console Amazon EC2. Pour plus d'informations, voir [Utilisation des instantanés locaux](#). Vous pouvez également automatiser le cycle de vie des instantanés locaux utilisant Amazon Data Lifecycle Manager. Pour plus d'informations, consultez [Automatisez les instantanés sur un Outpost](#).

6. Puis-je créer, utiliser ou supprimer des instantanés locaux si je Outpost perds la connectivité à sa région ?

Non La connectivité avec sa région est Outpost indispensable, car celle-ci fournit les services d'accès, d'autorisation, de journalisation et de surveillance essentiels à la santé de vos instantanés. S'il n'y a pas de connectivité, vous ne pouvez pas créer de nouveaux instantanés locaux, créer des volumes ou lancer des instances à partir d'instantanés locaux existants ou supprimer des instantanés locaux.

7. À quelle vitesse la capacité de stockage Amazon S3 est-elle disponible après la suppression des instantanés locaux ?

La capacité de stockage Amazon S3 est disponible 72 heures après la suppression des instantanés locaux et des volumes qui y font référence.

8. Comment puis-je m'assurer que la capacité Amazon S3 de mon ordinateur ne sera pas épuisée Outpost ?

Nous vous recommandons d'utiliser les CloudWatch alarmes Amazon pour surveiller la capacité de stockage de votre Amazon S3 et supprimer les instantanés et les volumes dont vous n'avez plus besoin afin d'éviter de manquer de capacité de stockage. Si vous utilisez Amazon Data Lifecycle Manager pour automatiser le cycle de vie des instantanés locaux, assurez-vous que vos politiques de conservation des instantanés ne conservent pas les instantanés plus longtemps que nécessaire.

9. Que se passe-t-il si je n'ai plus de capacité Amazon S3 locale sur un appareil Outpost ?

Si vous manquez de capacité Amazon S3 locale sur un Outpost, Amazon Data Lifecycle Manager ne sera pas en mesure de créer correctement des instantanés locaux sur le Outpost. Amazon Data Lifecycle Manager tentera de créer les instantanés locaux sur le Outpost, mais les instantanés passent immédiatement à l'état initial et ils sont finalement supprimés par Amazon Data Lifecycle Manager. Nous vous recommandons d'utiliser la CloudWatch métrique `SnapshotsCreateFailed` Amazon pour surveiller vos politiques de cycle de vie des instantanés afin de détecter les échecs liés à la création de snapshots. Pour plus d'informations, consultez [Surveillez les politiques du Data Lifecycle Manager à l'aide de CloudWatch](#).

10. Puis-je utiliser les instantanés locaux et les AMI sauvegardées par les instantanés locaux avec les instances Spot et le parc d'instances Spot ?

Non, vous ne pouvez pas utiliser les instantanés locaux ou les AMI sauvegardées par instantanés locaux pour lancer des instances Spot ou un parc d'instances Spot.

11. Puis-je utiliser les instantanés locaux et les AMI sauvegardées par instantanés locaux avec Amazon EC2 Auto Scaling ?

Oui, vous pouvez utiliser des instantanés locaux et des AMI soutenues par des instantanés locaux pour lancer des groupes Auto Scaling dans un sous-réseau qui se trouve sur le même Outpost site que les instantanés. Le rôle lié au service de groupe Amazon EC2 Auto Scaling doit être autorisé à utiliser la clé KMS utilisée pour chiffrer les instantanés.

Vous ne pouvez pas utiliser des instantanés locaux ou des AMI soutenues par des instantanés locaux pour lancer des groupes Auto Scaling dans une AWS région.

Conditions préalables

Pour stocker des instantanés sur un Outpost, vous devez en avoir un Outpost qui est provisionné avec S3 sur Outposts. Pour plus d'informations sur S3 on Outposts, consultez [S3 on Outposts](#) dans le guide de l'utilisateur Amazon S3 on Outposts.

Considérations

Gardez ce qui suit à l'esprit lorsque vous travaillez avec des instantanés locaux.

- Ils Outpost doivent disposer d'une connexion à leur AWS région pour utiliser les instantanés locaux.
- Les métadonnées de l'instantané sont stockées dans la AWS région associée au Outpost. Cela n'inclut pas les données d'instantanés.
- Les instantanés stockés sur un Outpost sont chiffrés par défaut. Les instantanés non chiffrés ne sont pas pris en charge. Lorsque vous créez un volume sur et Outpost à partir d'un instantané local, le volume est chiffré à l'aide de la même clé KMS que le cliché source. Vous pouvez toutefois modifier la clé de chiffrement lorsque vous copiez un instantané local.
- Une fois que vous avez supprimé des instantanés locaux d'un Outpost, la capacité de stockage Amazon S3 utilisée par les instantanés supprimés est disponible dans les 72 heures. Pour plus d'informations, consultez [Supprimer les instantanés locaux](#).
- Vous ne pouvez pas exporter des instantanés locaux à partir d'un Outpost.
- Vous ne pouvez pas activer la restauration rapide des instantanés pour les instantanés locaux.
- Les API directes EBS ne sont pas pris en charge par les instantanés locaux.
- Vous ne pouvez pas copier des instantanés locaux ou des AMI d'une région Outpost vers une AWS région, d'une région Outpost à une autre ou au sein d'un Outpost. Cependant, vous pouvez copier des instantanés d'une AWS région vers un Outpost. Pour plus d'informations, consultez [Copier des instantanés depuis une AWS De la région à Outpost](#).
- Lorsque vous copiez un instantané d'une AWS région vers un Outpost autre, les données sont transférées via la liaison de service. La copie simultanée de plusieurs instantanés peut avoir un impact sur les autres services exécutés sur le Outpost.
- Tu ne peux pas partager les instantanés locaux.

- Vous devez utiliser les politiques IAM pour vous assurer que vos exigences en matière de résidence des données sont respectées. Pour plus d'informations, consultez [Contrôle de l'accès avec IAM](#).
- Les Instantanés locaux sont des sauvegardes incrémentielles. Seuls les blocs du volume qui ont changé depuis votre instantané le plus récent sont enregistrés. Chaque instantané local contient toutes les informations nécessaires à la restauration de vos données (à partir du moment où l'instantané a été pris) sur un nouveau volume EBS. Pour plus d'informations, consultez [Comment fonctionnent les instantanés Amazon EBS](#).
- Vous ne pouvez pas utiliser les politiques IAM pour imposer la résidence des données CopySnapshot et les CopyImage actions.

Contrôle de l'accès avec IAM

Vous pouvez utiliser des politiques Gestion des identités et des accès AWS (IAM) pour contrôler les autorisations dont disposent les principaux utilisateurs (AWS comptes, utilisateurs IAM et rôles IAM) lorsqu'ils utilisent des instantanés locaux. Voici des exemples de politiques que vous pouvez utiliser pour accorder ou refuser l'autorisation d'effectuer des actions spécifiques avec les instantanés locaux.

Important

La copie d'instantanés et d'images depuis et Outpost vers une région n'est actuellement pas prise en charge. Par conséquent, vous ne pouvez actuellement pas utiliser les politiques IAM pour appliquer la résidence des données CopySnapshot et les CopyImage actions.

Rubriques

- [Appliquer la résidence des données pour les instantanés](#)
- [Empêcher les principaux de supprimer les instantanés locaux](#)

Appliquer la résidence des données pour les instantanés

L'exemple de politique suivant empêche tous les administrateurs de créer des instantanés à partir de volumes et d'instances et de stocker les données des instantanés dans une AWS région. Outpost
`arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef` Les

principaux peuvent toujours créer des instantanés locaux. Cette politique garantit que tous les instantanés restent sur le Outpost.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource": "arn:aws:ec2:us-east-1:snapshot/*",
      "Condition": {
        "StringEquals": {
          "ec2:SourceOutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0"
        },
        "Null": {
          "ec2:OutpostArn": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource": "*"
    }
  ]
}
```

Empêcher les principaux de supprimer les instantanés locaux

L'exemple de politique suivant empêche tous les administrateurs de supprimer les instantanés locaux qui sont stockés sur. Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

Utilisation des instantanés locaux

Les sections suivantes expliquent comment utiliser les instantanés locaux.

Rubriques

- [Règles de stockage des instantanés](#)

- [Créez des instantanés locaux à partir de volumes sur un Outpost](#)
- [Créer des AMI à partir d'instantanés locaux](#)
- [Copier des instantanés depuis un AWS De la région à Outpost](#)
- [Copier des AMI depuis un AWS De la région à Outpost](#)
- [Créer des volumes à partir d'instantanés locaux](#)
- [Lancer des instances à partir d'AMI sauvegardées par des instantanés locaux](#)
- [Supprimer les instantanés locaux](#)
- [Automatisez les instantanés sur un Outpost](#)

Règles de stockage des instantanés

Les règles suivantes s'appliquent au stockage des instantanés :

- Si l'instantané le plus récent d'un volume est stocké sur un Outpost, tous les instantanés suivants doivent être stockés sur le même Outpost.
- Si l'instantané le plus récent d'un volume est stocké dans une AWS région, tous les instantanés suivants doivent être stockés dans la même région. Pour commencer à créer des instantanés locaux à partir de ce volume, procédez comme suit :
 1. Créez un instantané du volume de la AWS région.
 2. Copiez la capture d'écran Outpost depuis la AWS région.
 3. Créez un volume à partir de l'instantané local.
 4. Attachez le volume à une instance sur le Outpost.

Pour le nouveau volume sur le Outpost, l'instantané suivant peut être stocké sur Outpost ou dans la AWS région. Tous les instantanés successifs doivent alors être stockés dans le même emplacement.

- Les instantanés locaux, y compris les instantanés créés sur une région Outpost et les instantanés copiés vers et Outpost depuis une AWS région, ne peuvent être utilisés que pour créer des volumes sur cette même région. Outpost
- Si vous créez un volume sur et Outpost à partir d'un instantané d'une région, tous les instantanés successifs de ce nouveau volume doivent se trouver dans la même région.
- Si vous créez un volume sur et Outpost à partir d'un instantané local, tous les instantanés successifs de ce nouveau volume doivent être identiques Outpost.

Créez des instantanés locaux à partir de volumes sur un Outpost

Vous pouvez créer des instantanés locaux à partir des volumes de votre Outpost. Vous pouvez choisir de stocker les instantanés sur le même volume Outpost que le volume source ou dans la région pour le Outpost.

Les instantanés locaux peuvent être utilisés pour créer des volumes Outpost uniquement sur le même support.

Pour plus d'informations, consultez [Créer des instantanés Amazon EBS](#)

Créer des AMI à partir d'instantanés locaux

Vous pouvez créer des Amazon Machine Images (AMI) en combinant des instantanés locaux et des instantanés stockés dans la région du Outpost. Par exemple, si vous avez une Outpost entrée us-east-1, vous pouvez créer une AMI contenant des volumes de données sauvegardés par des instantanés locaux Outpost, et un volume racine soutenu par un instantané dans la us-east-1 région.

Vous pouvez également créer une AMI directement à partir d'une instance sur et Outpost qui prend en charge les instantanés locaux. Les instantanés de sauvegarde créés pour l'AMI peuvent être stockés sur le même emplacement Outpost que l'instance ou dans sa région parente.

Note

- Vous ne pouvez pas créer d'AMI qui incluent des instantanés de sauvegarde stockés sur plusieurs Outposts.
- Les AMI qui sont soutenues par des instantanés locaux ne peuvent être utilisées Outpost que pour lancer des instances sur celles-ci.

Pour créer une AMI sur un Outpost à partir de photos prises dans une région

1. Copiez les instantanés de la région vers le Outpost. Pour plus d'informations, consultez [Copier des instantanés depuis un AWS De la région à Outpost](#).
2. Utilisez la console Amazon EC2 ou la [commande](#) register-image pour créer l'AMI à l'aide des copies instantanées du Outpost. Pour plus d'informations, consultez [Création d'une AMI à partir d'un instantané](#).

Pour créer une AMI directement à partir d'une instance sur un Outpost

Utilisez la [commande](#) `create-image` avec le `--snapshot-location` paramètre pour contrôler l'emplacement de stockage des captures d'écran :

- Pour stocker les instantanés localement sur le même emplacement Outpost que l'instance, spécifiez `local`.
- Pour stocker des instantanés dans la région parent du Outpost, spécifiez `regional`.

Si l'instance source se trouve sur une instance Outpost qui prend en charge les instantanés locaux, le `--snapshot-location` paramètre est obligatoire. Si vous l'omettez, la demande échoue avec une `InvalidParameterValue` erreur.

L'exemple suivant crée une AMI et stocke les instantanés de sauvegarde sur le même emplacement Outpost que l'instance.

```
aws ec2 create-image \  
  --instance-id i-1234567890abcdef0 \  
  --name "My Outpost image" \  
  --snapshot-location local
```

Pour créer une AMI dans une région à partir d'une instance d'un Outpost

Utilisez la [commande](#) `create-image` et spécifiez `regional` le `--snapshot-location` paramètre.

L'exemple suivant crée une AMI et stocke les instantanés de sauvegarde dans la région parent du Outpost.

```
aws ec2 create-image \  
  --instance-id i-1234567890abcdef0 \  
  --name "My Regional image" \  
  --snapshot-location regional
```

Copier des instantanés depuis un AWS De la région à Outpost

Vous pouvez copier des instantanés d'une AWS région vers une Outpost. Vous ne pouvez le faire que si les instantanés se trouvent dans la région pour le Outpost. Si les instantanés se trouvent dans une autre région, vous devez d'abord copier l'instantané dans la région pour le Outpost, puis le copier de cette région vers le Outpost.

 Note

Vous ne pouvez pas copier des instantanés locaux d'une région Outpost vers une région, d'une région Outpost à une autre ou au sein d'une même Outpost région.

Pour plus d'informations, consultez [Copier un instantané Amazon EBS](#).

Copier des AMI depuis un AWS De la région à Outpost

Vous pouvez copier des AMI d'une AWS région vers une Outpost. Lorsque vous copiez une AMI d'une région vers une Outpost, tous les instantanés associés à l'AMI sont copiés de la région vers la Outpost.

Vous ne pouvez copier une AMI d'une région vers une Outpost que si les instantanés associés à l'AMI se trouvent dans la région pour la Outpost. Si les instantanés se trouvent dans une autre région, vous devez d'abord copier l'AMI dans la région pour la Outpost, puis la copier de cette région vers la Outpost.

 Note

Vous ne pouvez pas copier une AMI d'une région Outpost vers une région, de l'une Outpost vers une autre ou au sein d'une Outpost.

Vous pouvez copier des AMI d'une région vers une Outpost à l'aide de la [AWS CLI commande](#) `copy-image` uniquement.

Créer des volumes à partir d'instantanés locaux

Vous pouvez créer des volumes sur et Outpost à partir d'instantanés locaux. Les volumes doivent être créés sur le même support Outpost que les instantanés sources. Vous ne pouvez pas utiliser des instantanés locaux pour créer des volumes dans la région pour la Outpost.

Lorsque vous créez un volume à partir d'un instantané local, vous ne pouvez pas rechiffrer le volume à l'aide d'une autre clé KMS. Les volumes créés à partir d'instantanés locaux doivent être chiffrés à l'aide de la même clé KMS que l'instantané source.

Pour plus d'informations, consultez [Créez un volume Amazon EBS](#).

Lancer des instances à partir d'AMI sauvegardées par des instantanés locaux

Vous pouvez lancer des instances à partir d'AMI qui sont sauvegardées par des instantanés locaux. Vous devez lancer les instances sur la même Outpost interface que l'AMI source. Pour plus d'informations, consultez la section [Lancer une instance sur vous Outpost](#) dans le Guide de AWS Outposts l'utilisateur.

Supprimer les instantanés locaux

Vous pouvez supprimer des instantanés locaux à partir d'unOutpost. Une fois que vous avez supprimé un instantané d'unOutpost, la capacité de stockage Amazon S3 utilisée par l'instantané supprimé est disponible dans les 72 heures suivant la suppression de l'instantané et des volumes qui font référence à cet instantané.

Étant donné que la capacité de stockage Amazon S3 n'est pas disponible immédiatement, nous vous recommandons d'utiliser CloudWatch les alarmes Amazon pour surveiller votre capacité de stockage Amazon S3. Supprimez les instantanés et les volumes dont vous n'avez plus besoin pour éviter de manquer de capacité de stockage.

Pour plus d'informations sur la suppression des instantanés, consultez [Suppression d'un instantané](#).

Automatisez les instantanés sur un Outpost

Vous pouvez créer des politiques de cycle de vie des instantanés Amazon Data Lifecycle Manager qui créent, copient, conservent et suppriment automatiquement des instantanés de vos volumes et instances sur unOutpost. Vous pouvez choisir de stocker les instantanés dans une région ou de les stocker localement sur unOutpost. En outre, vous pouvez copier automatiquement les instantanés créés et stockés dans une AWS région vers unOutpost.

Le tableau suivant donne un aperçu des fonctionnalités prises en charge.

Emplacement des ressources	Destination des instantanés	Cross-region copie vers la région	Cross-region copier vers Outpost	Restauration d'instantané rapide	Cross-account partage
Région	Région	✓	✓	✓	✓
Outpost	Région	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

Considérations

- Seules les politiques de cycle de vie des snapshots Amazon EBS sont actuellement prises en charge. EBS-backed Les politiques AML et les politiques Cross-account de partage d'événements ne sont pas prises en charge.
- Si une politique gère les instantanés pour les volumes ou les instances d'une Région, les instantanés sont créés dans la même Région que la ressource source.
- Si une politique gère les instantanés pour des volumes ou des instances sur unOutpost, des instantanés peuvent être créés sur la sourceOutpost, ou dans la région pour cela. Outpost
- Une seule politique ne peut pas gérer à la fois les instantanés d'une région et les instantanés d'une région. Outpost Si vous devez automatiser les instantanés dans une région et sur uneOutpost, vous devez créer des politiques distinctes.
- La restauration rapide des instantanés n'est pas prise en charge pour les instantanés créés sur unOutpost, ou pour les instantanés copiés sur un. Outpost
- Cross-account le partage n'est pas pris en charge pour les instantanés créés sur unOutpost.
- Pre-scripts et les post-scripts ne sont pas pris en charge pour les instantanés créés sur un. Outpost

Pour plus d'informations sur la création d'un cycle de vie des instantanés qui gère les instantanés locaux, consultez [Automatisation des cycles de vie des instantanés](#).

Instantanés locaux dans les zones locales

Les instantanés Amazon EBS sont une copie ponctuelle de vos volumes EBS.

Les instantanés des volumes EBS d'une zone AWS locale peuvent être stockés dans Amazon S3 dans la même zone locale ou dans la région parent de cette zone locale. Le stockage des instantanés dans une zone locale peut vous aider à répondre aux besoins de résidence des données en garantissant que les données des instantanés sont traitées et stockées dans un pays, un État ou une municipalité spécifique. Vous pouvez également configurer des politiques d'application de la résidence des données à l'aide d'IAM pour vous assurer que les données des instantanés ne quittent pas la zone locale.

Les zones locales sont idéales pour les applications qui nécessitent une latence d'une milliseconde à un chiffre ou un traitement de données local en rapprochant AWS l'infrastructure de vos utilisateurs finaux et de vos centres d'affaires. En outre, vous pouvez répondre aux exigences de résidence

des données pour les charges de travail sensibles à la réglementation et à la conformité. Pour plus d'informations, consultez [Qu'est-ce que AWS les zones locales](#) ?

Les instantanés locaux sont actuellement pris en charge dans les zones locales qui prennent en charge Amazon S3. Pour plus d'informations, consultez la section Fonctionnalités des zones [AWS locales](#).

Rubriques

- [Questions fréquentes \(FAQ\)](#)
- [Considérations](#)
- [Contrôle de l'accès avec IAM](#)

Questions fréquentes (FAQ)

1. Que sont les instantanés locaux dans les zones locales ?

Les instantanés locaux dans les zones locales sont des instantanés qui sont stockés dans Amazon S3 dans une zone locale. Par défaut, les instantanés des volumes Amazon EBS d'une zone locale sont stockés dans Amazon S3 dans la région parent. Si la zone locale prend en charge Amazon S3, vous pouvez choisir de stocker les instantanés localement dans la zone locale à la place. Tout comme les instantanés dans AWS les régions, les instantanés locaux dans les zones locales sont incrémentiels, ce qui signifie que seuls les blocs du volume qui ont été modifiés après votre dernier instantané sont enregistrés. Vous pouvez utiliser ces instantanés pour restaurer un volume Amazon EBS dans la même zone locale à tout moment.

2. Pourquoi utiliser les instantanés locaux ?

Utilisez les instantanés locaux dans les zones locales pour répondre aux exigences de résidence ou d'isolation des données en vous assurant que les données de vos instantanés se trouvent dans un emplacement géographique spécifique, tel qu'un pays, un État ou une municipalité.

3. Comment appliquer la résidence des données instantanées dans les zones locales ?

Vous pouvez utiliser des politiques Gestion des identités et des accès AWS (IAM) pour contrôler les autorisations dont disposent les responsables (AWS comptes, utilisateurs IAM et rôles IAM) lorsqu'ils travaillent avec des instantanés locaux dans des zones locales et pour appliquer la résidence des données. Par exemple, vous pouvez créer une politique qui empêche les utilisateurs de créer des instantanés à partir de volumes situés dans une zone locale et de stocker

ces instantanés dans une AWS région. Pour plus d'informations, consultez [Contrôle de l'accès avec IAM](#).

4. Les instantanés locaux multi-volumes et cohérents en cas de crash sont-ils pris en charge ?

Oui, vous pouvez créer des instantanés locaux multivolumes et cohérents en cas de crash dans des zones locales à partir d'instances situées dans une zone locale.

5. Comment créer des instantanés locaux dans les zones locales ?

Vous pouvez créer des instantanés locaux dans les zones locales manuellement à l'aide de la console Amazon EC2 AWS CLI ou de la console Amazon EC2. Pour plus d'informations, voir [Création d'un instantané d'un volume EBS](#). Vous pouvez également automatiser le cycle de vie des instantanés locaux dans les zones locales à l'aide d'Amazon Data Lifecycle Manager. Pour plus d'informations, voir [Création d'une politique personnalisée Amazon Data Lifecycle Manager pour les instantanés EBS](#).

6. Puis-je copier des instantanés locaux dans des zones locales ?

Oui, vous pouvez copier des instantanés d'une région vers une zone locale de la même région, d'une zone locale vers sa région et d'une zone locale vers une autre zone locale du même groupe de zones locales.

7. Comment puis-je restaurer des données à partir d'instantanés locaux dans les zones locales ?

Vous pouvez utiliser des instantanés locaux dans les zones locales pour créer des volumes Amazon EBS dans la même zone locale uniquement.

8. Comment les instantanés locaux dans les zones locales sont-ils chiffrés ?

Consultez [Chiffrement Amazon EBS dans les zones locales, les avant-postes et les zones de longueur d'onde](#) la section Comportement du Zone-specific chiffrement local. Dans les zones locales où les ressources Amazon EBS sont chiffrées par défaut, les volumes créés à partir d'instantanés locaux sont toujours chiffrés à l'aide de la même AWS KMS clé que l'instantané. Vous pouvez toutefois modifier la clé de chiffrement lorsque vous copiez un instantané local.

9. Puis-je créer des EBS-backed AMI à l'aide d'instantanés locaux dans les zones locales ?

Oui, vous pouvez utiliser les instantanés locaux dans les zones locales lors de la création d'EBS-backed AMI en spécifiant la destination des instantanés comme zones locales. Pour plus d'informations, consultez [Créer une EBS-backed AMI Amazon](#).

10. Puis-je partager des instantanés locaux dans les zones locales ?

Oui, vous pouvez partager des instantanés locaux dans les zones locales avec d'autres AWS comptes qui ont activé l'utilisation de la zone locale dans leur compte.

11. Puis-je créer un instantané local d'un volume, puis passer à la création d'instantanés dans la région parent ?

Non, après avoir créé un instantané local d'un volume, vous ne pouvez pas créer de clichés successifs de ce volume dans la région parent. Étant donné que tous les instantanés sont incrémentiels, si l'instantané le plus récent d'un volume est un instantané local, tous les instantanés successifs de ce volume doivent être des instantanés locaux.

Considérations

Gardez les points suivants à l'esprit lorsque vous utilisez des instantanés locaux dans les zones locales.

- Les instantanés locaux sont actuellement pris en charge dans les zones locales qui prennent en charge Amazon S3.
- Les fonctionnalités suivantes ne peuvent pas être utilisées avec les instantanés locaux dans les zones locales :
 - Import/Export Actions relatives aux machines virtuelles
 - Restauration d'instantané rapide
 - API EBS Direct
 - Corbeille
 - Archive des instantanés
- Vous devez utiliser les politiques IAM pour appliquer vos exigences en matière de résidence des données. Pour plus d'informations, consultez [Contrôle de l'accès avec IAM](#).
- Si l'instantané le plus récent d'un volume est un instantané local, tous les instantanés suivants doivent être des instantanés locaux. De même, si l'instantané le plus récent d'un volume est stocké dans une AWS région, tous les instantanés successifs doivent être stockés dans la même région.

Contrôle de l'accès avec IAM

Vous pouvez utiliser des politiques Gestion des identités et des accès AWS (IAM) pour contrôler les autorisations dont disposent les principaux utilisateurs (AWS comptes, utilisateurs IAM et rôles IAM)

lorsqu'ils utilisent des instantanés locaux dans les zones locales. Voici des exemples de politiques que vous pouvez utiliser pour accorder ou refuser l'autorisation d'effectuer des actions spécifiques avec des instantanés locaux dans des zones locales.

Rubriques

- [Appliquer la résidence des données pour les instantanés locaux dans les zones locales](#)
- [Empêcher le partage des instantanés locaux dans les zones locales](#)
- [Empêcher les administrateurs de supprimer des instantanés locaux dans les zones locales](#)

Appliquer la résidence des données pour les instantanés locaux dans les zones locales

L'exemple de politique suivant limite les utilisateurs à créer uniquement des instantanés locaux dans des zones locales à partir de volumes et d'instances d'une zone locale. Il empêche les utilisateurs de créer des instantanés dans une région à partir de volumes et d'instances d'une zone locale.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:Location": "regional",
          "ec2:SourceAvailabilityZone": "local_zone"
        }
      }
    }
  ],
}
```

```

    {
      "Effect": "Deny",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:SourceAvailabilityZone": "local_zone"
        },
        "Null": {
          "ec2:Location": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource": "*"
    }
  ]
}

```

Empêcher le partage des instantanés locaux dans les zones locales

L'exemple de politique suivant empêche tous les utilisateurs de partager des instantanés locaux dans les zones locales.

JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "DenySnapshotModifyInLocalZone",
    "Effect": "Deny",
    "Action": [
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*::snapshot/*",
    "Condition": {
      "StringEquals": {
        "ec2:AvailabilityZone": "use1-atl2-az1"
      }
    }
  },
  {
    "Sid": "AllowSnapshotModifyElsewhere",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*::snapshot/*"
  }
]
```

Empêcher les administrateurs de supprimer des instantanés locaux dans les zones locales

L'exemple de politique suivant empêche tous les utilisateurs de supprimer des instantanés locaux dans les zones locales.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenySnapshotDeleteInLocalZone",
```

```
    "Effect": "Deny",
    "Action": [
      "ec2:DeleteSnapshot"
    ],
    "Resource": "arn:aws:ec2:*::snapshot/*",
    "Condition": {
      "StringEquals": {
        "ec2:AvailabilityZone": "use1-atl2-az1"
      }
    }
  },
  {
    "Sid": "AllowSnapshotDeleteElsewhere",
    "Effect": "Allow",
    "Action": [
      "ec2:DeleteSnapshot"
    ],
    "Resource": "arn:aws:ec2:*::snapshot/*"
  }
]
```

Chiffrement Amazon EBS

Utilisez le chiffrement Amazon EBS comme solution de chiffrement simple pour vos ressources Amazon EBS associées à vos instances Amazon EC2. Avec le chiffrement Amazon EBS, vous n'avez pas besoin de créer, de maintenir ou de sécuriser votre propre infrastructure de gestion des clés. Le chiffrement Amazon EBS utilise les clés AWS KMS keys lors de la création de volumes et d'instantanés chiffrés.

Les opérations de chiffrement se produisent sur les serveurs qui hébergent des instances EC2, assurant la sécurité des données au repos et des données en transit entre une instance et le stockage EBS associé.

Vous pouvez attacher simultanément des volumes chiffrés et des volumes non chiffrés à une instance. Tous les types d'instances Amazon EC2 prennent en charge le chiffrement Amazon EBS.

Table des matières

- [Comment fonctionne le chiffrement Amazon EBS](#)
- [Chiffrement Amazon EBS dans les zones locales, les avant-postes et les zones de longueur d'onde](#)
- [Exigences relatives au chiffrement Amazon EBS](#)
- [Activer le chiffrement Amazon EBS par défaut](#)
- [Chiffrer les ressources EBS](#)
- [Rotate \(Faire pivoter\) AWS KMS clés utilisées pour le chiffrement Amazon EBS](#)
- [Exemples de chiffrement Amazon EBS](#)

Comment fonctionne le chiffrement Amazon EBS

Vous pouvez chiffrer à la fois les volumes de démarrage et de données d'une instance EC2.

Lorsque vous créez un volume EBS chiffré et l'attachez à un type d'instance pris en charge, les types de données suivants sont chiffrés :

- Données au repos à l'intérieur du volume
- Toutes les données circulant entre le volume et l'instance
- Tous les instantanés créés à partir du volume

- Tous les volumes créés à partir de ces instantanés

Amazon EBS chiffre votre volume à l'aide d'une clé de données à l'[aide d'un chiffrement](#) des données conforme aux normes de l'industrie AES-256 . La clé de données est générée AWS KMS puis chiffrée à l' AWS KMS aide d'une AWS KMS clé avant d'être stockée avec les informations de votre volume. Amazon EBS crée automatiquement une ressource unique Clé gérée par AWS dans chaque région où vous créez des ressources Amazon EBS. L'[alias](#) de la clé KMS est `aws/ebs`. Par défaut, Amazon EBS utilise cette clé KMS pour le chiffrement. Vous pouvez également utiliser une clé de chiffrement symétrique gérée par le client que vous créez. L'utilisation de votre propre clé KMS vous donne plus de flexibilité dans la mesure où elle vous permet de créer des clés Clés KMS, de les modifier ou de les désactiver à votre convenance.

Amazon EC2 fonctionne avec AWS KMS pour chiffrer et déchiffrer vos volumes EBS de manière légèrement différente selon que l'instantané à partir duquel vous créez un volume chiffré est chiffré ou non chiffré.

Fonctionnement du chiffrement EBS lorsque le snapshot est chiffré

Lorsque vous créez un volume chiffré à partir d'un instantané chiffré dont vous êtes propriétaire, Amazon EC2 utilise Amazon EC2 AWS KMS pour chiffrer et déchiffrer vos volumes EBS comme suit :

1. Amazon EC2 envoie une [GenerateDataKeyWithoutPlaintext](#) demande à AWS KMS, en spécifiant la clé KMS que vous avez choisie pour le chiffrement des volumes.
2. Si le volume est chiffré à l'aide de la même clé KMS que le snapshot, AWS KMS utilise la même clé de données que le snapshot et le chiffre sous cette même clé KMS. Si le volume est chiffré à l'aide d'une autre clé KMS, AWS KMS génère une nouvelle clé de données et la chiffre avec la clé KMS que vous avez spécifiée. La clé de données chiffrée est envoyée à Amazon EBS pour être stockée avec les métadonnées du volume.
3. Lorsque vous associez le volume chiffré à une instance, Amazon EC2 envoie une [CreateGrant](#) demande à AWS KMS afin qu'il puisse déchiffrer la clé de données.
4. AWS KMS déchiffre la clé de données chiffrée et envoie la clé de données déchiffrée à Amazon EC2.
5. Amazon EC2 utilise la clé de données en texte brut du matériel Nitro pour chiffrer le disque sur I/O le volume. La clé de données en texte brut est conservée en mémoire tant que le volume est attaché à l'instance.

Fonctionnement du chiffrement EBS lorsque l'instantané est non chiffré

Lorsque vous créez un volume chiffré à partir d'un instantané non chiffré, Amazon EC2 fonctionne avec AWS KMS pour chiffrer et déchiffrer vos volumes EBS comme suit :

1. Amazon EC2 envoie une [CreateGrant](#) demande à AWS KMS, afin qu'il puisse chiffrer le volume créé à partir de l'instantané.
2. Amazon EC2 envoie une [GenerateDataKeyWithoutPlaintext](#) demande à AWS KMS, en spécifiant la clé KMS que vous avez choisie pour le chiffrement des volumes.
3. AWS KMS génère une nouvelle clé de données, la chiffre sous la clé KMS que vous avez choisie pour le chiffrement du volume et envoie la clé de données chiffrée à Amazon EBS pour qu'elle soit stockée avec les métadonnées du volume.
4. Amazon EC2 envoie une [demande de](#) déchiffrement AWS KMS à pour déchiffrer la clé de données chiffrée, qu'il utilise ensuite pour chiffrer les données du volume.
5. Lorsque vous associez le volume chiffré à une instance, Amazon EC2 envoie une [CreateGrant](#) demande à AWS KMS, afin qu'il puisse déchiffrer la clé de données.
6. Lorsque vous associez le volume chiffré à une instance, Amazon EC2 envoie une [demande de](#) déchiffrement à AWS KMS, en spécifiant la clé de données chiffrée.
7. AWS KMS déchiffre la clé de données chiffrée et envoie la clé de données déchiffrée à Amazon EC2.
8. Amazon EC2 utilise la clé de données en texte brut du matériel Nitro pour chiffrer le disque sur I/O le volume. La clé de données en texte brut est conservée en mémoire tant que le volume est attaché à l'instance.

Pour plus d'informations, consultez [Comment Amazon Elastic Block Store \(Amazon EBS\) utilise AWS KMS](#) et [Amazon EC2, exemple deux](#) dans le Guide du développeur AWS Key Management Service .

Comment les clés KMS inutilisables affectent les clés de données

Lorsqu'une clé KMS devient inutilisable, l'effet est presque immédiat (sous réserve d'une éventuelle cohérence). L'état de clé de la clé KMS change pour refléter son nouvel état, et toutes les requêtes d'utilisation de la clé KMS dans des opérations cryptographiques échouent.

Lorsque vous effectuez une action qui rend la clé KMS inutilisable, il n'y a aucun effet immédiat sur l'instance EC2 ou sur les volumes EBS attachés. Amazon EC2 utilise la clé de données, et non la clé KMS, pour chiffrer tous les disques I/O lorsque le volume est attaché à l'instance.

Toutefois, lorsque le volume EBS chiffré est détaché de l'instance EC2, Amazon EBS supprime la clé de données en texte brut du matériel Nitro. La prochaine fois que le volume EBS chiffré est attaché à une instance EC2, l'attachement échoue, car Amazon EBS ne peut pas utiliser la clé KMS pour déchiffrer la clé de données chiffrée du volume. Pour utiliser le volume EBS à nouveau, vous devez rendre la clé KMS à nouveau utilisable.

Tip

Si vous ne souhaitez plus accéder aux données stockées dans un volume EBS chiffré à l'aide d'une clé de données générée à partir d'une clé KMS que vous souhaitez rendre inutilisable, nous vous recommandons de détacher le volume EBS de l'instance EC2 avant de rendre la clé KMS inutilisable.

Pour plus d'informations, veuillez consulter la rubrique [How unusable KMS keys affect data keys](#) dans le Guide du développeur AWS Key Management Service .

Chiffrement Amazon EBS dans les zones locales, les avant-postes et les zones de longueur d'onde

Le comportement de chiffrement d'Amazon EBS varie en fonction du type d'emplacement dans lequel vous créez vos ressources.

Local Zones

Dans les zones locales suivantes, toutes les ressources Amazon EBS sont chiffrées par défaut. Vous ne pouvez pas créer de volumes ou d'instantanés non chiffrés. Si vous ne spécifiez pas de clé KMS, Amazon EBS chiffre vos ressources avec la clé de chiffrement par défaut de votre compte. Par défaut, il s'agit du Clé gérée par AWS (aws/ebs). Pour modifier la clé de chiffrement par défaut de votre compte, consultez [Clé de chiffrement par défaut](#).

- Amérique du Nord : us-east-1-atl-1a,us-east-1-bos-1a,us-east-1-chi-1a,us-east-1-dfw-1a,us-east-1-iah-1a,us-east-1-mci-1a,us-east-1-mia-1a,us-east-1-msp-1a,us-east-1-nyc-1a,us-east-1-phl-1a,us-east-1-qro-1a,us-east-2-mci-1a,us-east-2-mci-1b,us-west-2-den-1a,us-west-2-hnl-1a,us-west-2-las-1a,us-west-2-las-1b,us-west-2-pdx-1a,us-west-2-phx-1a, us-west-2-sea-1a

- Asie-Pacifique : ap-northeast-1-tpe-1a,,ap-south-1-ccu-1a, ap-south-1-ccu-2a,ap-south-1-del-1a,ap-south-1-del-2a,ap-southeast-1-bkk-1a,ap-southeast-1-han-1a,ap-southeast-1-mnl-1a,ap-southeast-2-akl-1a, ap-southeast-2-per-1a
- Europe : eu-central-1-ath-1a,eu-central-1-ham-1a,eu-central-1-ist-1a,eu-central-1-waw-1a,eu-north-1-cph-1a, eu-north-1-hel-1a
- Amérique du Sud : us-east-1-bue-1a,us-east-1-lim-1a, us-east-1-scl-1a
- Moyen-Orient : me-south-1-mct-1a
- Afrique : af-south-1-los-1a

Dans toutes les autres zones locales, le chiffrement Amazon EBS suit le même comportement que dans la région parente.

Avant-postes et zones de longueur d'onde

Toutes les ressources Amazon EBS sur AWS Outposts et dans les zones de longueur d'onde sont chiffrées par défaut. Vous ne pouvez pas créer de volumes ou d'instantanés non chiffrés. Si vous ne spécifiez pas de clé KMS, Amazon EBS chiffre vos ressources avec la clé de chiffrement par défaut de votre compte. Par défaut, il s'agit du Clé gérée par AWS (aws/ebs). Pour modifier la clé de chiffrement par défaut de votre compte, consultez [Clé de chiffrement par défaut](#).

Lorsque vous créez un volume à partir d'un instantané local dans ces zones, le volume est chiffré à l'aide de la même clé KMS que le cliché source. Vous pouvez toutefois modifier la clé de chiffrement lorsque vous copiez un instantané local.

Exigences relatives au chiffrement Amazon EBS

Avant de commencer, vérifiez que les conditions requises suivantes sont respectées :

Exigences

- [Types de volume pris en charge](#)
- [Types d'instance pris en charge](#)
- [Autorisations pour les utilisateurs](#)
- [Autorisations pour les instances](#)

Types de volume pris en charge

Le chiffrement est pris en charge par tous les types de volume EBS. Les mêmes performances IOPS sont à prévoir sur les volumes chiffrés que sur les volumes non chiffrés, avec des conséquences minimales sur la latence. Vous pouvez accéder à des volumes chiffrés de la même façon qu'à des volumes non chiffrés. Le chiffrement et le déchiffrement sont gérés de façon transparente et ne nécessitent aucune action supplémentaire de votre part ou de vos applications.

Types d'instance pris en charge

Le chiffrement Amazon EBS est disponible sur tous les types d'[instances de génération actuelle et de génération précédente](#).

Autorisations pour les utilisateurs

Lorsque vous utilisez une clé KMS pour le chiffrement EBS, la politique de clé KMS permet à tout utilisateur ayant accès aux AWS KMS actions requises d'utiliser cette clé KMS pour chiffrer ou déchiffrer les ressources EBS. Vous devez accorder aux utilisateurs l'autorisation d'appeler les actions suivantes afin d'utiliser le chiffrement EBS :

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`

Tip

Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour permettre à l'utilisateur de créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée pour le compte de l'utilisateur par un AWS service, comme illustré dans l'exemple suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": [
        "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-a123b4cd56ef"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

Pour plus d'informations, voir [Autoriser l'accès au AWS compte et activer les politiques IAM](#) dans la section Politiques clé par défaut du Guide du AWS Key Management Service développeur.

Autorisations pour les instances

Lorsqu'une instance tente d'interagir avec une AMI, un volume ou un instantané chiffré, une autorisation de clé KMS est attribuée au rôle réservé à l'identité de l'instance. Le rôle réservé à l'identité est un rôle IAM utilisé par l'instance pour interagir avec des AMI, des volumes ou des instantanés chiffrés en votre nom.

Identity-only les rôles n'ont pas besoin d'être créés ou supprimés manuellement et aucune politique ne leur est associée. De plus, vous ne pouvez pas accéder aux informations d'identification du rôle réservé à l'identité.

Note

Identity-only les rôles ne sont pas utilisés par les applications de votre instance pour accéder à d'autres ressources AWS KMS chiffrées, telles que des objets Amazon S3 ou des tables Dynamo DB. Ces opérations sont effectuées à l'aide des informations d'identification d'un

rôle d'instance Amazon EC2 ou d'autres AWS informations d'identification que vous avez configurées sur votre instance.

Identity-only les rôles sont soumis aux politiques de contrôle des [services](#) (SCP) et aux politiques [clés](#) KMS. Si une clé SCP ou KMS refuse qu'un rôle réservé à l'identité accède à une clé KMS, il est possible que vous ne parveniez pas à lancer des instances EC2 avec des volumes chiffrés ou à l'aide d'AMI ou d'instantanés chiffrés.

Si vous créez une politique SCP ou clé qui refuse l'accès en fonction de la localisation du réseau à l'aide des clés de condition `aws:SourceIp` `aws:VpcSourceIp` `aws:SourceVpc`, ou `aws:SourceVpce` AWS globales, vous devez vous assurer que ces déclarations de politique ne s'appliquent pas aux rôles d'instance uniquement. Pour obtenir des exemples de stratégies, consultez la section [Exemples de stratégies relatives aux périmètres de données](#) (français non garanti).

Identity-only Les ARN de rôle utilisent le format suivant :

```
arn:aws-partition:iam::account_id:role/aws:ec2-infrastructure/instance_id
```

Lorsqu'une attribution de clé est attribuée à une instance, elle est attribuée à la session à rôle assumé spécifique à cette instance. L'ARN principal du bénéficiaire utilise le format suivant :

```
arn:aws-partition:sts::account_id:assumed-role/aws:ec2-infrastructure/instance_id
```

Activer le chiffrement Amazon EBS par défaut

Vous pouvez configurer votre AWS compte pour appliquer le chiffrement des nouveaux volumes EBS et des copies instantanées que vous créez. Par exemple, Amazon EBS chiffre les volumes EBS créés lorsque vous lancez une instance et les instantanés que vous copiez à partir d'un instantané non chiffré. Pour voir des exemples de transition de ressources EBS non chiffrées à chiffrées, consultez [Chiffrer les ressources non chiffrées](#).

Le chiffrement par défaut n'a aucun effet sur les instantanés ni les volumes EBS existants.

Considérations

- Le chiffrement par défaut est un Region-specific paramètre. Si vous l'activez pour une région, vous ne pouvez pas le désactiver pour certains volumes ou instantanés spécifiques dans cette région.

- Le chiffrement Amazon EBS est pris en charge par défaut sur tous les types d'[instances de génération actuelle et de génération précédente](#).
- Si vous copiez un instantané et le chiffrez dans une nouvelle clé KMS, une copie complète (non incrémentielle) est créée. Cela entraîne des coûts de stockage supplémentaires.

Console

Pour activer le chiffrement par défaut pour une région

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région.
3. Dans le volet de navigation, sélectionnez Paramètres, puis sélectionnez l'onglet Protection et sécurité des données.
4. Dans la section Chiffrement EBS, choisissez Gérer.
5. Sélectionnez Activer. Vous conservez le Clé gérée par AWS avec l'alias aws/ebs créé en votre nom comme clé de cryptage par défaut, ou vous choisissez une clé de cryptage symétrique gérée par le client.
6. Choisissez Mettre à jour le chiffrement EBS.

AWS CLI

Pour afficher le paramètre de chiffrement par défaut

Utilisez la commande [get-ebs-encryption-by-default](#).

- Pour une région spécifique

```
aws ec2 get-ebs-encryption-by-default --region region
```

- Pour toutes les régions de votre compte

```
echo -e "Region      \t Encrypt \t Key"; \  
echo -e "----- \t ----- \t -----" ; \  
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].  
[RegionName]" --output text);  
do  
    default=$(aws ec2 get-ebs-encryption-by-default --region $region --query  
    "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
```



```
kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
'.KmsKeyId');
echo -e "$region \t $default \t\t $kms_key";
done
```

Pour activer le chiffrement par défaut

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/enable-ebs-encryption-by-default.html> `enable-ebs-encryption-by-default`.

- Pour une région spécifique

```
aws ec2 enable-ebs-encryption-by-default --region region
```

- Pour toutes les régions de votre compte

```
echo -e "Region \t Encrypt \t Key"; \
echo -e "----- \t ----- \t -----" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 enable-ebs-encryption-by-default --region $region --query
"{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
'.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

Pour désactiver le chiffrement par défaut

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/disable-ebs-encryption-by-default.html> `disable-ebs-encryption-by-default`.

- Pour une région spécifique

```
aws ec2 disable-ebs-encryption-by-default --region region
```

- Pour toutes les régions de votre compte

```
echo -e "Region \t Encrypt \t Key"; \
```

```

echo -e "----- \t ----- \t -----" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 disable-ebs-encryption-by-default --region $region --query
"{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
'.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done

```

PowerShell

Pour afficher le paramètre de chiffrement par défaut

Utilisez l'applet de commande [Get-EC2EbsEncryptionByDefault](#).

- Pour une région spécifique

```
Get-EC2EbsEncryptionByDefault -Region region
```

- Pour toutes les régions de votre compte

```

(Get-EC2Region).RegionName |
    ForEach-Object {
        [PSCustomObject]@{
            Region = $_
            EC2EbsEncryptionByDefault = Get-EC2EbsEncryptionByDefault -Region $_
            EC2EbsDefaultKmsKeyId = Get-EC2EbsDefaultKmsKeyId -Region $_
        } } |
    Format-Table -AutoSize

```

Pour activer le chiffrement par défaut

Utilisez l'applet de commande [Enable-EC2EbsEncryptionByDefault](#).

- Pour une région spécifique

```
Enable-EC2EbsEncryptionByDefault -Region region
```

- Pour toutes les régions de votre compte

```
(Get-EC2Region).RegionName |
  ForEach-Object {
    [PSCustomObject]@{
      Region                        = $_
      EC2EbsEncryptionByDefault = Enable-EC2EbsEncryptionByDefault -Region $_
      EC2EbsDefaultKmsKeyId      = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } |
  Format-Table -AutoSize
```

Pour désactiver le chiffrement par défaut

Utilisez l'applet de commande [Disable-EC2EbsEncryptionByDefault](#).

- Pour une région spécifique

```
Disable-EC2EbsEncryptionByDefault -Region region
```

- Pour toutes les régions de votre compte

```
(Get-EC2Region).RegionName |
  ForEach-Object {
    [PSCustomObject]@{
      Region                        = $_
      EC2EbsEncryptionByDefault = Disable-EC2EbsEncryptionByDefault -Region $_
      EC2EbsDefaultKmsKeyId      = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } |
  Format-Table -AutoSize
```

Vous ne pouvez pas modifier la clé KMS associée à un snapshot ou à un volume chiffré existant. Toutefois, vous pouvez associer une autre clé KMS pendant une opération de copie d'instantané, de sorte que l'instantané copié obtenu soit chiffré par cette nouvelle clé KMS.

Clé de chiffrement par défaut

Amazon EBS crée automatiquement une ressource unique Clé gérée par AWS dans chaque région où vous créez des ressources Amazon EBS. L'alias de cette clé KMS est `aws/ebs`. Il s'agit de votre clé de chiffrement par défaut. Vous pouvez remplacer la clé de chiffrement par défaut par une clé gérée par le client.

Pour modifier la clé de chiffrement par défaut pour une région, utilisez l'une des méthodes suivantes.

Console

Pour modifier la clé de chiffrement par défaut pour une région

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, sélectionnez la région.
3. Dans le volet de navigation, sélectionnez Paramètres, puis sélectionnez l'onglet Protection et sécurité des données.
4. Dans la section Chiffrement EBS, choisissez Gérer.
5. Pour Clé de chiffrement par défaut, sélectionnez l'ID de clé KMS que vous souhaitez utiliser.
6. Choisissez Mettre à jour le chiffrement EBS.

AWS CLI

Utilisez la commande [modify-ebs-default-kms-key-id](#).

```
aws ec2 modify-ebs-default-kms-key-id --kms-key-id key-id --region region
```

PowerShell

Utilisez l'applet de commande [Edit-EC2EbsDefaultKmsKeyId](#).

```
Edit-EC2EbsDefaultKmsKeyId -KmsKeyId key-id -Region region
```

Chiffrer les ressources EBS

Vous chiffrez les volumes EBS en activant le chiffrement, soit en utilisant le [chiffrement par défaut](#), soit en activant le chiffrement lorsque vous créez un volume que vous souhaitez chiffrer.

Lorsque vous chiffrez un volume, vous pouvez spécifier la clé de chiffrement KMS symétrique à utiliser à cette fin. Si vous ne spécifiez pas de clé KMS, la clé KMS utilisée pour le chiffrement dépend de l'état de chiffrement de l'instantané source et de son propriétaire. Pour plus d'informations, consultez le [tableau des résultats de chiffrement](#).

 Note

Si vous utilisez l'API ou AWS CLI pour spécifier une clé KMS, sachez que l' AWS authentification de la clé KMS est asynchrone. Si vous spécifiez un ID de clé KMS, un alias ou un ARN qui n'est pas valide, l'action peut sembler se terminer mais finalement échouer.

Vous ne pouvez pas modifier la clé KMS associée à un volume ou à un instantané existant.

Toutefois, vous pouvez associer une autre clé KMS pendant une opération de copie d'instantané, de sorte que l'instantané copié obtenu soit chiffré par cette nouvelle clé KMS.

Chiffrer un volume vide lors de sa création

Lorsque vous créez un volume EBS vide, vous pouvez le chiffrer en activant le chiffrement pour l'opération de création du volume spécifique. Si vous avez activé le chiffrement EBS par défaut, le volume est automatiquement chiffré à l'aide de votre clé KMS par défaut de chiffrement EBS. Sinon, vous pouvez spécifier une autre clé de chiffrement KMS symétrique pour l'opération de création du volume spécifique. Le volume est chiffré dès sa mise à disposition afin que vos données soient toujours sécurisées. Pour connaître les procédures détaillées, consultez [Créez un volume Amazon EBS](#).

Par défaut, la clé KMS que vous avez sélectionnée lors de la création d'un volume chiffre les instantanés que vous créez à partir de ce volume, et les volumes que vous restaurez à partir de ces instantanés chiffrés. Vous ne pouvez pas supprimer le chiffrement d'un volume ou d'un instantané chiffré, ce qui signifie qu'un volume restauré à partir d'un instantané chiffré, ou une copie d'un instantané chiffré, reste toujours chiffré(e).

Les instantanés publics de volumes chiffrés ne sont pas pris en charge. Vous pouvez cependant partager un instantané chiffré avec certains comptes. Pour obtenir des instructions complètes, consultez [Partager un instantané Amazon EBS avec d'autres AWS comptes](#).

Chiffrer les ressources non chiffrées

Vous ne pouvez pas chiffrer directement les volumes ou les instantanés non chiffrés existants.

Pour chiffrer un volume non chiffré, créez un instantané de ce volume, puis utilisez-le pour créer un nouveau volume chiffré. Pour plus d'informations, consultez [Créer des instantanés](#) et [Créer un volume](#).

Pour chiffrer un instantané non chiffré, créez une copie chiffrée de cet instantané. Pour plus d'informations, consultez [Copie d'un instantané](#).

Si vous activez le chiffrement de votre compte par défaut, les volumes et les copies d'instantanés créés à partir de clichés non chiffrés sont toujours chiffrés. Dans le cas contraire, vous devez spécifier les paramètres de chiffrement dans la demande. Pour plus d'informations, consultez [Activer le chiffrement par défaut](#).

Rotate (Faire pivoter) AWS KMS clés utilisées pour le chiffrement Amazon EBS

Les bonnes pratiques de chiffrement décourage la réutilisation étendue des clés de chiffrement.

Pour créer un nouveau matériel cryptographique à utiliser avec le chiffrement Amazon EBS, vous pouvez soit créer une nouvelle clé gérée par le client, puis modifier vos applications pour utiliser cette nouvelle clé KMS. Vous pouvez également activer la rotation automatique des clés pour une clé gérée par le client existante.

Lorsque vous activez la rotation automatique des clés pour une clé gérée par le client, vous AWS KMS générez chaque année de nouveaux éléments cryptographiques pour la clé KMS. AWS KMS enregistre toutes les versions précédentes du matériel cryptographique afin que vous puissiez continuer à déchiffrer et à utiliser les volumes et les instantanés précédemment chiffrés avec ce matériel clé KMS. AWS KMS ne supprime aucun élément clé pivoté tant que vous n'avez pas supprimé la clé KMS.

Lorsque vous utilisez une clé gérée par le client modifiée pour chiffrer un nouveau volume ou un nouvel instantané, AWS KMS utilise la (nouvelle) clé actuelle. Lorsque vous utilisez une clé gérée par le client modifiée pour déchiffrer un volume ou un instantané, elle AWS KMS utilise la version du matériel cryptographique qui a été utilisée pour le chiffrer. Si un volume ou un instantané est chiffré avec une version précédente du matériel cryptographique, continuez AWS KMS à utiliser cette version précédente pour le déchiffrer. AWS KMS ne rechiffre pas les volumes ou les instantanés précédemment chiffrés pour utiliser le nouveau matériel cryptographique après une rotation de clé. Ils restent cryptés avec le matériel cryptographique avec lequel ils ont été chiffrés à l'origine. Vous pouvez utiliser en toute sécurité une clé gérée par le client modifiée dans les applications et les AWS services sans modifier le code.

 Note

- La rotation automatique des touches n'est prise en charge que pour les clés symétriques gérées par le client et dont le contenu clé est AWS KMS créé.
- AWS KMS change automatiquement Clés gérées par AWS chaque année. Vous ne pouvez pas activer ou désactiver la rotation des clés pour Clés gérées par AWS.

Pour plus d'informations, consultez [Rotation de clé KMS](#) dans le Guide du développeur AWS Key Management Service .

Exemples de chiffrement Amazon EBS

Lorsque vous créez une ressource EBS chiffrée, elle est chiffrée par la clé KMS par défaut de chiffrement EBS de votre compte, sauf si vous spécifiez une autre clé gérée par le client dans les paramètres de création de volume ou le mappage de périphérique de stockage en mode bloc pour l'AMI ou l'instance.

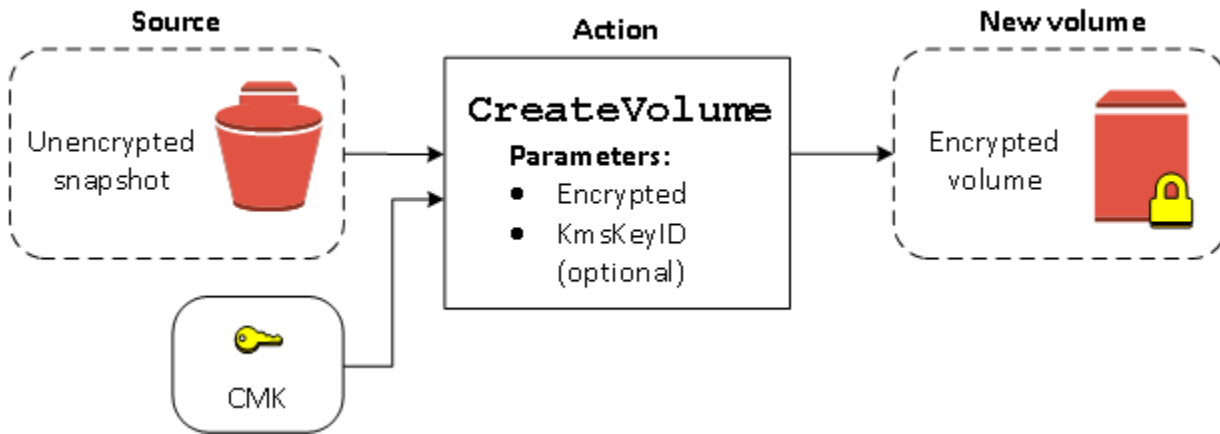
Les exemples suivants montrent comment vous pouvez gérer l'état de chiffrement de vos volumes et instantanés. Pour obtenir une liste complète des cas de chiffrement, consultez le [tableau des résultats de chiffrement](#).

Exemples

- [Restauration d'un volume non chiffré \(chiffrement par défaut non activé\)](#)
- [Restauration d'un volume non chiffré \(chiffrement par défaut activé\)](#)
- [Copie d'un instantané non chiffré \(chiffrement par défaut non activé\)](#)
- [Copie d'un instantané non chiffré \(chiffrement par défaut activé\)](#)
- [Re-encrypt un volume chiffré](#)
- [Re-encrypt un instantané chiffré](#)
- [Migration des données entre les volumes chiffrés et non chiffrés](#)
- [Résultats du chiffrement](#)

Restauration d'un volume non chiffré (chiffrement par défaut non activé)

Sans le chiffrement par défaut activé, un volume restauré à partir d'un instantané non chiffré est non chiffré par défaut. Cependant, vous pouvez chiffrer le volume créé en définissant le paramètre `Encrypted` et, éventuellement, le paramètre `KmsKeyId`. Le schéma suivant illustre le processus.

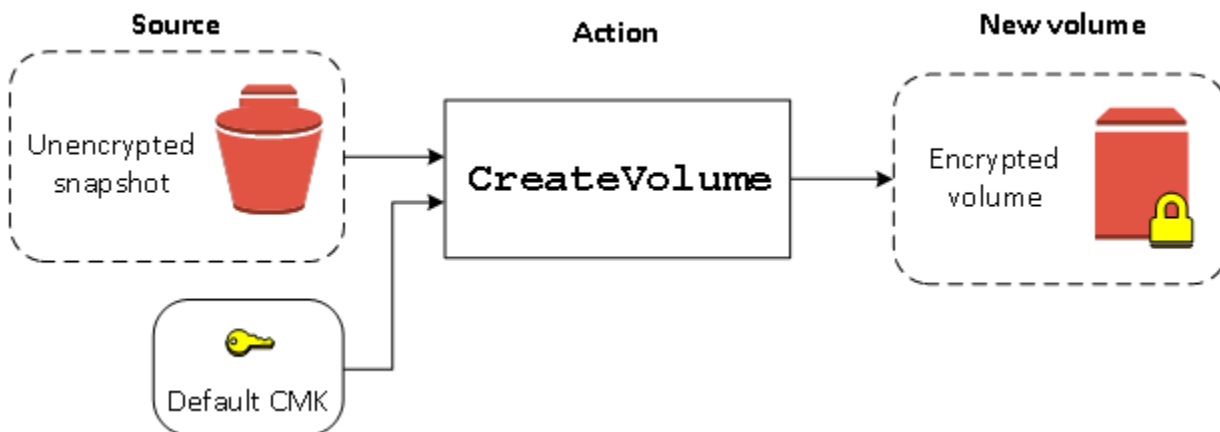


Si vous ne spécifiez pas le paramètre `KmsKeyId`, le volume obtenu est chiffré à l'aide de votre clé KMS par défaut de chiffrement EBS. Vous devez fournir un ID de clé KMS pour chiffrer le volume avec une autre clé KMS.

Pour plus d'informations, consultez [Créez un volume Amazon EBS](#).

Restauration d'un volume non chiffré (chiffrement par défaut activé)

Lorsque vous avez activé le chiffrement par défaut, le chiffrement est obligatoire pour les volumes restaurés à partir d'instantanés non chiffrés et aucun paramètre de chiffrement n'est requis pour utiliser votre clé KMS par défaut. Le schéma suivant illustre ce cas simple par défaut :

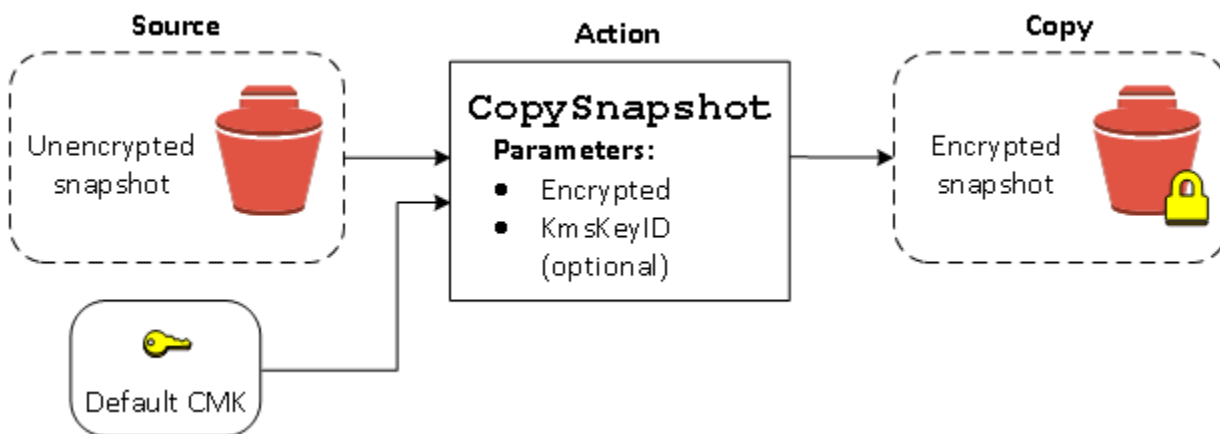


Si vous souhaitez chiffrer le volume restauré avec une clé de chiffrement gérée par le client symétrique, vous devez fournir les paramètres `Encrypted` et `KmsKeyId`, comme illustré dans [Restauration d'un volume non chiffré \(chiffrement par défaut non activé\)](#).

Copie d'un instantané non chiffré (chiffrement par défaut non activé)

Sans le chiffrement par défaut activé, une copie d'un instantané non chiffré est non chiffrée par défaut. Cependant, vous pouvez chiffrer l'instantané créé en définissant le paramètre `Encrypted` et, éventuellement, le paramètre `KmsKeyId`. Si vous omettez le paramètre `KmsKeyId`, l'instantané obtenu est chiffré par votre clé KMS par défaut. Vous devez fournir un ID de clé KMS pour chiffrer le volume avec une autre clé de chiffrement KMS symétrique.

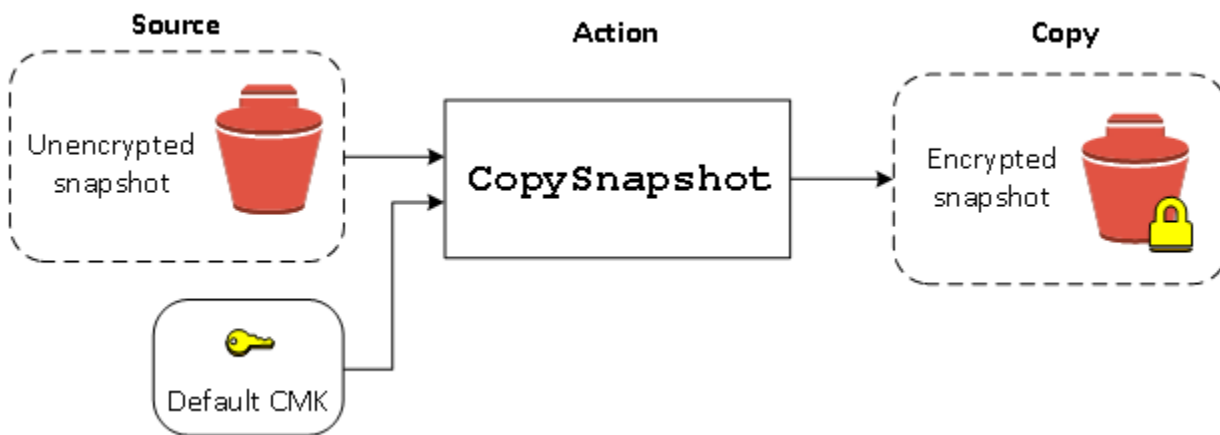
Le schéma suivant illustre le processus.



Vous pouvez chiffrer un volume EBS en copiant un instantané non chiffré sur un instantané chiffré, puis en créant un volume à partir de l'instantané chiffré. Pour plus d'informations, consultez [Copier un instantané Amazon EBS](#).

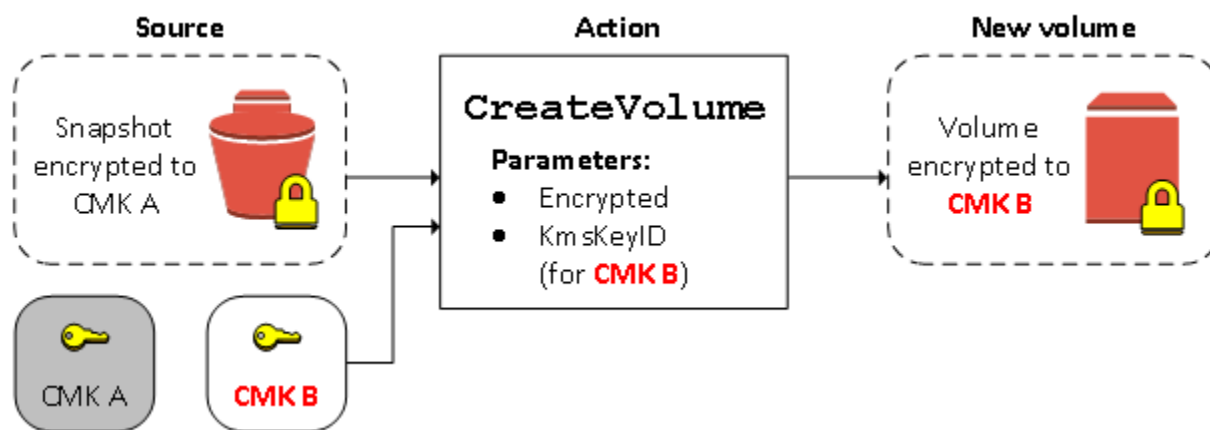
Copie d'un instantané non chiffré (chiffrement par défaut activé)

Lorsque vous avez activé le chiffrement par défaut, le chiffrement est obligatoire pour les copies d'instances non chiffrées et aucun paramètre de chiffrement n'est requis si votre clé KMS par défaut est utilisée. Le schéma suivant illustre ce scénario par défaut :



Re-encrypt un volume chiffré

Lorsque l'action `CreateVolume` est effectuée sur un instantané chiffré, vous avez l'option de rechiffrer celui-ci avec une autre clé clé KMS. Le schéma suivant illustre le processus. Dans cet exemple, vous possédez deux clés Clés KMS, la clé KMS A et la clé KMS B. L'instantané source est chiffré avec la clé KMS A. Pendant la création de volume, avec l'ID clé KMS de la clé KMS B spécifié comme paramètre, les données sources sont automatiquement déchiffrées, puis rechiffrées avec la clé KMS B.

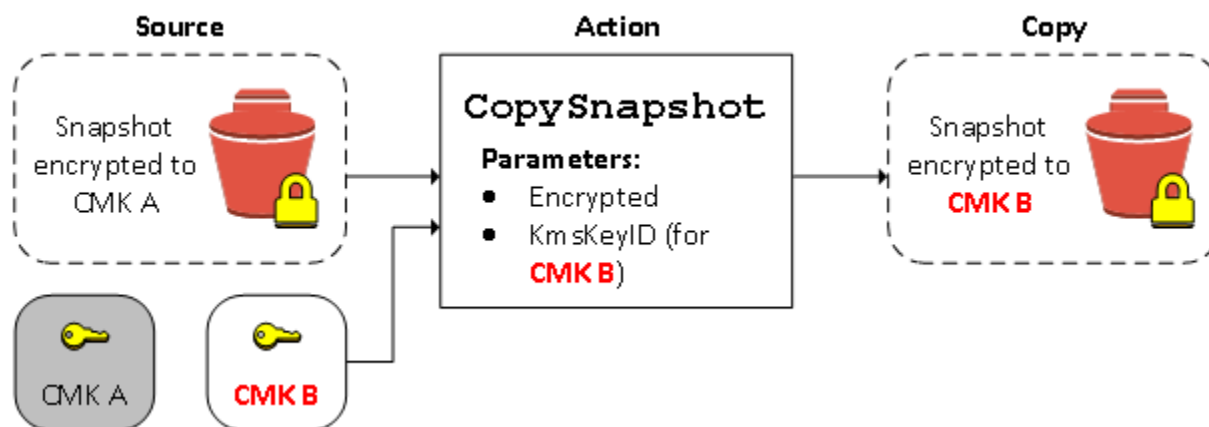


Pour plus d'informations, consultez [Créez un volume Amazon EBS](#).

Re-encrypt un instantané chiffré

La possibilité de chiffrer un instantané pendant la copie vous permet d'appliquer une nouvelle clé de chiffrement KMS symétrique à un instantané déjà chiffré que vous possédez. Les volumes restaurés à partir de la copie qui en résulte sont uniquement accessibles à l'aide de la nouvelle clé KMS. Le schéma suivant illustre le processus. Dans cet exemple, vous possédez deux clés Clés KMS, la clé KMS A et la clé KMS B. L'instantané source est chiffré avec la clé KMS A. Pendant la copie, avec

l'ID clé KMS de la clé KMS B spécifié comme paramètre, les données sources sont automatiquement rechiffrées avec la clé KMS B.



Dans un scénario similaire, vous pouvez choisir d'appliquer de nouveaux paramètres de chiffrement à une copie d'instantané partagée avec vous. Par défaut, la copie est chiffrée avec une clé KMS partagée par le propriétaire de l'instantané. Toutefois, nous vous recommandons de créer une copie de l'instantané partagé sous une clé KMS différente de celle dont vous avez le contrôle. Cela protège votre accès au volume si la clé KMS d'origine est compromise ou si le propriétaire la révoque pour quelque raison que ce soit. Pour plus d'informations, consultez [Chiffrement et copie d'instantanés](#).

Migration des données entre les volumes chiffrés et non chiffrés

Lorsque vous avez accès à la fois à un volume chiffré et non chiffré, vous pouvez librement transférer des données entre eux. EC2 effectue les opérations de chiffrement et de déchiffrement en toute transparence.

Instances Linux

Par exemple, utilisez la commande `rsync` pour copier les données. Dans l'exemple suivant, les données source se trouvent à l'emplacement `/mnt/source` et le volume de destination est monté à l'emplacement `/mnt/destination`.

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

instances Windows

Par exemple, utilisez la commande `robocopy` pour copier les données. Dans l'exemple suivant, les données source se trouvent à l'emplacement `D:\` et le volume de destination est monté à l'emplacement `E:\`.

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

Nous vous conseillons d'utiliser des dossiers plutôt que de copier tout un volume, afin d'éviter d'éventuels problèmes de dossiers masqués.

Résultats du chiffrement

Le tableau suivant décrit le résultat du chiffrement pour chaque combinaison possible de paramètres.

Le chiffrement EBS est-il activé ?	Le chiffrement par défaut est-il activé ?	Source du volume	Par défaut (aucune clé gérée par le client n'est spécifiée)	Personnalisé (clé gérée par le client spécifiée)
Non	Non	Nouveau volume (vide)	Non chiffré	N/A
Non	Non	Instantané non chiffré que vous possédez	Non chiffré	
Non	Non	Instantané chiffré que vous possédez	Chiffré par la même clé	
Non	Non	Instantané non chiffré qui est partagé avec vous	Non chiffré	
Non	Non	Instantané chiffré qui est partagé avec vous	Chiffré par clé gérée par le client par défaut*	
Oui	Non	Nouveau volume	Chiffré par défaut par clé gérée par le client	Chiffré par une clé gérée par le client spécifiée**
Oui	Non	Instantané non chiffré que vous possédez	Chiffré par défaut par clé gérée par le client	

Le chiffrement EBS est-il activé ?	Le chiffrement par défaut est-il activé ?	Source du volume	Par défaut (aucune clé gérée par le client n'est spécifiée)	Personnalisé (clé gérée par le client spécifiée)
Oui	Non	Instantané chiffré que vous possédez	Chiffré par la même clé	
Oui	Non	Instantané non chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Oui	Non	Instantané chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Non	Oui	Nouveau volume (vide)	Chiffré par défaut par clé gérée par le client	N/A
Non	Oui	Instantané non chiffré que vous possédez	Chiffré par défaut par clé gérée par le client	
Non	Oui	Instantané chiffré que vous possédez	Chiffré par la même clé	
Non	Oui	Instantané non chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Non	Oui	Instantané chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Oui	Oui	Nouveau volume	Chiffré par défaut par clé gérée par le client	Chiffré par une clé gérée par le client spécifiée

Le chiffrement EBS est-il activé ?	Le chiffrement par défaut est-il activé ?	Source du volume	Par défaut (aucune clé gérée par le client n'est spécifiée)	Personnalisé (clé gérée par le client spécifiée)
Oui	Oui	Instantané non chiffré que vous possédez	Chiffré par défaut par clé gérée par le client	
Oui	Oui	Instantané chiffré que vous possédez	Chiffré par la même clé	
Oui	Oui	Instantané non chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Oui	Oui	Instantané chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	

* Il s'agit de la clé gérée par le client par défaut utilisée pour le chiffrement EBS du AWS compte et de la région. Par défaut, il s'agit d'une clé unique Clé gérée par AWS pour EBS, ou vous pouvez spécifier une clé gérée par le client.

** Il s'agit d'une clé gérée par le client spécifiée pour le volume au moment du lancement. Cette clé gérée par le client est utilisée à la place de la clé gérée par le client par défaut pour le AWS compte et la région.

Performances volumiques d'Amazon EBS

Plusieurs facteurs, notamment I/O les caractéristiques et la configuration de vos instances et volumes, peuvent affecter les performances d'Amazon EBS. Si vous suivez les instructions figurant sur nos pages détaillées des produits Amazon EBS et Amazon EC2, vous obtiendrez généralement de bonnes performances. Cependant, dans certains cas, vous devrez peut-être effectuer quelques réglages pour obtenir des performances optimales. Nous vous recommandons d'optimiser les performances à l'aide des informations provenant de votre charge de travail réelle, en plus des comparaisons, afin de déterminer votre configuration optimale. Après avoir appris les bases de l'utilisation des volumes EBS, il est conseillé d'examiner les I/O performances dont vous avez besoin et les options qui s'offrent à vous pour améliorer les performances d'Amazon EBS afin de répondre à ces exigences.

AWS les mises à jour des performances des types de volumes EBS peuvent ne pas avoir d'effet immédiat sur vos volumes existants. Pour bénéficier de performances optimales sur un ancien volume, vous devrez peut-être d'abord effectuer une action `ModifyVolume` sur celui-ci. Pour de plus amples informations, veuillez consulter [Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes](#).

Table des matières

- [Conseils sur les performances Amazon EBS](#)
- [Optimisation Amazon EBS](#)
- [Initialiser les volumes Amazon EBS](#)
- [Pondération configurable de la bande passante des instances](#)
- [I/O Caractéristiques et surveillance d'Amazon EBS](#)
- [Configuration Amazon EBS et RAID](#)
- [Volumes Amazon EBS de référence](#)

Conseils sur les performances Amazon EBS

Ces conseils constituent des bonnes pratiques à appliquer pour obtenir des performances optimales à partir de vos volumes EBS, dans différents scénarios d'utilisation.

Utiliser des EBS-optimized instances

Sur les instances ne prenant pas en charge le EBS-optimized débit, le trafic réseau peut être confronté au trafic entre votre instance et vos volumes EBS ; sur les EBS-optimized instances, les deux types de trafic sont séparés. Certaines configurations d' EBS-optimized instance entraînent un coût supplémentaire (telles que C3, R3 et M3), tandis que d'autres sont toujours gratuites EBS-optimized (telles que M4, C4, C5 et D2). Pour de plus amples informations, veuillez consulter [Optimisation Amazon EBS](#).

Configurer la bande passante de l'instance

Pour les types d'instances pris en charge, vous pouvez configurer la pondération de la bande passante de l'instance afin d'augmenter la bande passante Amazon EBS de 25 % à l'aide de la pondération de la ebs-1 bande passante. Cette fonctionnalité vous permet d'optimiser l'allocation des ressources réseau de votre instance entre le réseau EBS et le réseau VPC, améliorant ainsi potentiellement les performances d'EBS pour les charges de travail. I/O-intensive Pour de plus amples informations, veuillez consulter [Pondération configurable de la bande passante des instances](#).

Comprendre comment les performances sont calculées

Lorsque vous mesurez les performances de vos volumes EBS, il est important de comprendre les unités de mesure impliquées et la méthode de calcul des performances. Pour plus d'informations, consultez [I/O Caractéristiques et surveillance d'Amazon EBS](#).

Comprendre votre charge de travail

Il existe un lien entre les performances maximales de vos volumes EBS, la taille et le nombre d' I/O opérations et le temps nécessaire à l'exécution de chaque action. Chacun de ces facteurs (performances et latence) influe sur les autres, et les différentes applications sont plus sensibles à un facteur ou à un autre. I/O Pour de plus amples informations, veuillez consulter [Volumes Amazon EBS de référence](#).

Être conscient des pertes de performances lors de l'initialisation des volumes à partir d'instantanés

La latence augmente considérablement la première fois que vous accédez à chaque bloc de données sur un nouveau volume EBS créé à partir d'un instantané. Vous pouvez éviter cette baisse de performances à l'aide de l'une des solutions suivantes :

- Accédez à chaque bloc avant de placer le volume en production. Ce processus est appelé initialisation (anciennement « préchauffage »). Pour de plus amples informations, veuillez consulter [Initialiser manuellement les volumes après leur création](#).
- Activez la restauration rapide d'un instantané sur un instantané pour vous assurer que les volumes EBS créés à partir de celui-ci sont entièrement initialisés lors de la création et fournissent instantanément toutes leurs performances provisionnées. Pour de plus amples informations, veuillez consulter [Restauration d'instantané rapide Amazon EBS](#).

Facteurs qui peuvent dégrader les performances des volumes HDD

Lorsque vous créez un instantané d'un volume HDD à débit optimisé (st1) ou HDD à froid (sc1), les performances peuvent diminuer jusqu'à la valeur de référence du volume pendant que l'instantané est en cours de création. Ce comportement est propre à ces types de volume. Parmi les autres facteurs susceptibles de limiter les performances, citons l'augmentation du débit que l'instance peut prendre en charge, la baisse des performances rencontrée lors de l'initialisation des volumes créés à partir d'un instantané et la présence excessive de petites quantités aléatoires I/O sur le volume. Pour plus d'informations sur le calcul du débit des volumes HDD, consultez [Types de volume Amazon EBS](#).

Vos performances peuvent également être affectées si votre application n'envoie pas suffisamment de I/O demandes. Cela peut être contrôlé en examinant la longueur et la I/O taille de la file d'attente de votre volume. La longueur de la file d'attente correspond au nombre de I/O demandes en attente depuis votre application vers votre volume. Pour une cohérence maximale, les HDD-backed volumes doivent maintenir une longueur de file d'attente (arrondie au nombre entier le plus proche) de 4 ou plus lors de l'exécution séquentielle I/O de 1 Mio. Pour plus d'informations sur la façon d'assurer la cohérence des performances de vos volumes, consultez [I/O Caractéristiques et surveillance d'Amazon EBS](#).

Augmentez la lecture anticipée pour les charges de travail à haut débit et à lecture intensive sur st1 et sc1 (Instances Linux uniquement)

Certaines charges de travail impliquent une forte densité de lecture et accèdent au périphérique de stockage en mode bloc via le cache d'une page du système d'exploitation (par exemple, à partir d'un système de fichiers). Dans ce cas, afin d'obtenir un débit optimal, nous vous recommandons de configurer le paramètre de lecture anticipée sur 1 Mio. Il s'agit d'un paramètre par périphérique de stockage en mode bloc, qui ne s'applique qu'à vos volumes HDD.

Afin d'examiner la valeur actuelle de lecture anticipée pour vos périphériques de stockage en mode bloc, utilisez la commande suivante :

```
$ sudo blockdev --report /dev/<device>
```

Les informations sur les périphériques de stockage en mode bloc s'affichent au format suivant :

R0	RA	SSZ	BSZ	StartSec	Size	Device
rw	256	512	4096	4096	8587820544	/dev/<device>

Le périphérique affiché indique une valeur de lecture anticipée de 256 (la valeur par défaut). Multipliez ce nombre par la taille du secteur (512 octets) afin d'obtenir la taille de la mémoire tampon de lecture anticipée (128 Kio ici). Pour définir la valeur de la mémoire tampon sur 1 Mio, utilisez la commande suivante :

```
$ sudo blockdev --setra 2048 /dev/<device>
```

Pour vérifier que le paramètre de lecture anticipée affiche maintenant 2 048, exécutez de nouveau la première commande.

N'utilisez ce paramètre que lorsque votre charge de travail est séquentielle I/Os et importante. S'il s'agit principalement de petits paramètres aléatoires I/Os, ce paramètre dégradera en fait vos performances. En général, si votre charge de travail est principalement limitée ou aléatoire I/Os, vous devriez envisager d'utiliser un volume SSD à usage général (gp2etgp3) plutôt qu'un sc1 volume st1 ou.

Utilisez un noyau Linux moderne (Instances Linux uniquement)

Utilisez un noyau Linux récent avec une prise en charge des descripteurs indirects. Tous les noyaux Linux version 3.8 et supérieures les prennent en charge, ainsi que toute instance EC2 de la génération actuelle. Si votre I/O taille moyenne est égale ou proche de 44 Ko, vous utilisez peut-être une instance ou un noyau qui ne prend pas en charge les descripteurs indirects. Pour plus d'informations sur la dérivation de la I/O taille moyenne à partir CloudWatch des statistiques Amazon, consultez [I/O Caractéristiques et surveillance d'Amazon EBS](#).

Pour obtenir un débit optimal sur les volumes st1 ou sc1, nous vous recommandons d'appliquer la valeur 256 au paramètre `xen_blkfront.max` (pour les versions de noyau Linux antérieures à la 4.6) ou au paramètre `xen_blkfront.max_indirect_segments` (pour un noyau Linux version 4.6

et supérieures). Le paramètre approprié peut être défini dans la ligne de commande de démarrage de votre système d'exploitation.

Par exemple, dans une AMI Amazon Linux avec un noyau antérieur, vous pouvez l'ajouter à la fin de la ligne du noyau, dans la configuration GRUB disponible dans `/boot/grub/menu.lst`:

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0  
xen_blkfront.max=256
```

Pour un noyau plus récent, la commande serait semblable à ce qui suit :

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0  
xen_blkfront.max_indirect_segments=256
```

Redémarrez votre instance pour que ce paramètre prenne effet.

Pour plus d'informations, voir [Configurer GRUB pour les AMI paravirtuelles](#). D'autres distributions Linux, en particulier celles qui n'utilisent pas le programme d'amorçage GRUB, peuvent nécessiter une approche différente pour le réglage des paramètres du noyau.

Pour plus d'informations sur les I/O caractéristiques d'EBS, consultez la présentation [Amazon EBS : Designing for Performance](#) re:Invent sur ce sujet.

Utiliser RAID 0 pour optimiser l'utilisation des ressources d'instance

Certains types d'instances peuvent générer I/O un débit supérieur à celui que vous pouvez provisionner pour un seul volume EBS. Vous pouvez associer plusieurs volumes dans une configuration RAID 0 afin d'utiliser la bande passante disponible pour ces instances. Pour de plus amples informations, veuillez consulter [Configuration Amazon EBS et RAID](#).

Surveillez les performances des volumes Amazon EBS

Vous pouvez surveiller et analyser les performances de vos volumes Amazon EBS à l'aide d'Amazon CloudWatch, des contrôles de statut et des statistiques de performances détaillées d'EBS. Pour plus d'informations, consultez [Statistiques CloudWatch Amazon pour Amazon EBS](#) et [Statistiques de performances détaillées d'Amazon EBS](#).

Optimisation Amazon EBS

Une instance optimisée pour Amazon EBS utilise une pile de configuration optimisée et fournit une capacité dédiée supplémentaire à Amazon EBS. I/O Cette optimisation fournit les meilleures performances pour vos volumes EBS en minimisant les conflits entre Amazon EBS I/O et le reste du trafic provenant de votre instance.

Les instances optimisées par EBS fournissent une bande passante dédiée vers Amazon EBS. En cas d'attachement à une instance optimisée pour EBS :

- **io2** Les volumes Block Express sont conçus pour fournir une latence moyenne inférieure à 500 microsecondes pour des opérations de 16 Ko I/O . **io2** Les volumes Block Express offrent également une meilleure latence aux valeurs aberrantes par rapport aux volumes à usage général, réduisant ainsi de plus de 10 fois la fréquence des I/Os dépassements de 800 microsecondes. **io1** et les **io2** volumes sont conçus pour fournir au moins 90 % de leurs performances IOPS provisionnées 99,9 % du temps au cours d'une année donnée.
- **gp2** et les **gp3** volumes sont conçus pour fournir au moins 90 % de leurs performances IOPS provisionnées 99 % du temps au cours d'une année donnée.
- **st1** et les **sc1** volumes fournissent au moins 90 % de leurs performances de débit attendues 99 % du temps au cours d'une année donnée.

Non-compliant les périodes sont réparties de manière approximativement uniforme, ciblant 99 % du débit total attendu chaque heure. Pour de plus amples informations, veuillez consulter [Types de volume Amazon EBS](#).

La I/O taille de votre charge de travail aura un impact sur la latence moyenne observée, car la latence augmente avec l'augmentation de I/O la taille. Par exemple, les volumes **io2** Block Express sont conçus pour fournir une latence moyenne inférieure à 500 microsecondes pour des opérations de 16 Ko I/O .

Pour plus d'informations, veuillez consulter la rubrique [Instances optimisées pour Amazon EBS](#) dans le Guide de l'utilisateur Amazon EC2.

Initialiser les volumes Amazon EBS

Lorsque vous créez un volume Amazon EBS, que ce soit à partir d'un instantané EBS ou d'un autre volume EBS (copie du volume), les blocs de données doivent être écrits sur le volume pour que vous puissiez y accéder. Pour les volumes créés à partir d'instants, les blocs de données doivent être

téléchargés depuis Amazon S3 vers le nouveau volume. Pour les copies de volume, les blocs de données doivent être copiés du volume source vers la copie du volume. Ce processus est appelé initialisation du volume. Pendant ce temps, le volume en cours d'initialisation peut connaître une I/O latence accrue et des performances réduites. Les performances du volume complet ne sont atteintes que lorsque tous les blocs de stockage ont été téléchargés et écrits sur le volume.

 Note

Les volumes vides offrent des performances optimales immédiatement après leur création et ne nécessitent pas d'initialisation.

Le taux d'initialisation du volume par défaut fluctue tout au long du processus d'initialisation, ce qui peut rendre les délais d'exécution imprévisibles. Pour minimiser les impacts sur les performances associés à l'initialisation des volumes, vous pouvez utiliser les options suivantes :

Rubriques

- [Utiliser un tarif provisionné par Amazon EBS pour l'initialisation des volumes](#)
- [Utiliser un instantané activé pour une restauration rapide](#)
- [Initialiser manuellement les volumes après leur création](#)
- [Surveiller l'état de l'initialisation du volume Amazon EBS](#)

 Note

Le tarif provisionné Amazon EBS pour l'initialisation des volumes et la restauration rapide des instantanés ne sont pas pris en charge pour les copies en volume. Pour plus d'informations, voir Initialisation [de la copie de](#) volume.

Utiliser un tarif provisionné par Amazon EBS pour l'initialisation des volumes

Lorsque vous créez un volume Amazon EBS à partir d'un instantané, vous pouvez éventuellement spécifier un taux provisionné Amazon EBS pour l'initialisation du volume (taux d'initialisation du volume) compris entre 100 et 300. MiB/s Si vous spécifiez un taux d'initialisation du volume, les blocs de snapshots sont téléchargés depuis Amazon S3 et écrits sur le volume au rythme spécifié après leur création. Cela vous permet de créer des volumes entièrement initialisés et pleinement performants dans un laps de temps prévisible.

L'utilisation d'un taux d'initialisation des volumes est particulièrement utile lorsque vous créez plusieurs volumes simultanément et que vous devez tous les initialiser dans un laps de temps prévisible.

 Note

Le tarif provisionné Amazon EBS pour l'initialisation des volumes est pris en charge avec tous les types de volumes Amazon EBS et tous les types d'instances Amazon EC2, y compris les instances Amazon EC2 Mac.

Vous pouvez spécifier un taux d'initialisation du volume :

- Pour les demandes de création de volumes individuels
- Pour les mappages de périphériques à blocs de volume EBS dans les demandes de lancement d'instance
- Pour les mappages de périphériques à blocs de volume EBS dans les modèles de lancement
- Pour les volumes EBS créés par des tâches de remplacement du volume racine
- Pour les volumes EBS sur les clusters Amazon EKS (créés par EBS CSI Driver) et les clusters Amazon ECS

Rubriques

- [Comment ça marche](#)
- [Considérations](#)
- [Quotas](#)
- [Facturation](#)
- [Spécifier un taux d'initialisation du volume](#)

Comment ça marche

Lorsque vous créez un volume avec un taux d'initialisation du volume, les blocs de snapshots sont téléchargés depuis Amazon S3 vers le volume au rythme que vous spécifiez.

Le temps nécessaire pour initialiser le volume dépend des éléments suivants :

- La taille des données de capture instantanée, et non la taille du volume en cours de création.

 Tip

Pour connaître la taille des données d'un instantané, vérifiez le `FullSnapshotSizeInBytes` champ dans la sortie de la [commande](#) `describe-snapshots` ou le champ `Taille` complète de l'instantané dans la console.

- Le taux d'initialisation du volume que vous spécifiez

Par exemple, si vous créez un volume de 20 Go à l'aide d'un instantané contenant 10 Go de données et que vous spécifiez un taux d'initialisation du volume de 300 MiB/s, le volume sera complètement initialisé en 34,1 secondes environ ($10 \text{ GiB} / 300 = 34,1 \text{ secondes}$). De même, si vous créez 10 volumes avec le même snapshot et le même taux d'initialisation des volumes simultanément, les 10 volumes seront entièrement initialisés en 34,1 secondes.

Considérations

- Vous pouvez spécifier un taux d'initialisation du volume compris entre 100 et 300 MiB/s.
- Lorsque vous spécifiez un taux d'initialisation de volume, les frais et le délai de traitement sont basés sur la taille des données de capture instantanée (et non sur la taille du volume) et sur le taux que vous spécifiez. Pour de plus amples informations, veuillez consulter [Facturation](#).
- Amazon EBS fournit un taux moyen inférieur à 10 % du taux d'initialisation du volume que vous spécifiez pendant 99 % du temps.
- Si vous spécifiez un taux d'initialisation du volume et que vous utilisez un instantané pour lequel la restauration d'instantané rapide est activée, Amazon EBS utilise le taux spécifié au lieu de la restauration d'instantané rapide. Pour utiliser plutôt la restauration d'instantané rapide, ne spécifiez pas de taux d'initialisation du volume.
- Si Amazon EBS ne parvient pas à initialiser le volume au taux d'initialisation spécifié en raison de contraintes de capacité ou parce que vous avez dépassé votre [quota](#), la demande échoue.
- Vous ne pouvez pas spécifier de taux d'initialisation des volumes pour les volumes créés sur AWS Outposts, ou dans des zones locales ou des zones de longueur d'onde.

Quotas

Le taux cumulé d'initialisation MiB/s des volumes que vous pouvez demander pour des demandes de création de volumes simultanées est limité à 5 000. Par exemple, vous pouvez effectuer 50

demandes de création de volume simultanées avec un taux de 100 MiB/s (50 demandes simultanées * 100 MiB/s), ou 25 demandes simultanées avec un taux de 200 MiB/s (25 demandes simultanées * MiB/s taux 200). Cette limite s'applique par région. Si une demande dépasse cette limite, elle échoue. Attendez que certaines des demandes en cours soient traitées ou demandez une augmentation de quota. Pour de plus amples informations, veuillez consulter [Quotas pour Amazon EBS](#).

Facturation

Lorsque vous créez un volume avec un taux d'initialisation du volume, un tarif par Go vous est facturé en fonction du niveau d'initialisation sélectionné. Le taux varie selon les régions. Pour déterminer le tarif pour le niveau d'initialisation que vous avez sélectionné, ouvrez la tarification [Amazon EBS](#), sélectionnez votre région et accédez à la section Tarif provisionné pour l'initialisation des volumes.

Vous êtes facturé en fonction de la taille complète des données de l'instantané, et non de la taille du volume. Par exemple, si vous créez un instantané d'un volume de 100 Go contenant 50 Go de données écrites, la taille complète des données de l'instantané est de 50 Go. Si vous utilisez cet instantané pour créer un volume et spécifier un taux d'initialisation du volume, vos frais sont basés sur 50 GiB.

Tip

Pour connaître la taille complète des données de l'instantané, vérifiez le `FullSnapshotSizeInBytes` champ dans la sortie de la [commande](#) `describe-snapshots` ou le champ `Taille` complète de l'instantané dans la console.

La formule est la suivante :

Rate for the selected initialization tier in the Region × full snapshot data size

Le montant total vous est facturé dès que le volume entre dans l'active état. Les demandes échouées ne sont pas facturées.

Si vous supprimez un volume avant la fin de l'initialisation, le taux d'initialisation du volume demandé vous est toujours facturé.

Spécifier un taux d'initialisation du volume

Utilisez l'une des méthodes suivantes pour créer un volume à partir d'un instantané avec un taux d'initialisation du volume.

Console

Pour créer un de volumes

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Volumes, puis sélectionnez Créer un volume.
3. Pour Volume type (Type de volume), choisissez le type de volume à créer.
4. Dans Taille, entrez une taille égale ou supérieure à la taille du volume de l'instantané source.
5. Pour Zone de disponibilité, choisissez la zone de disponibilité dans laquelle créer le volume.
6. Pour Snapshot ID, sélectionnez l'instantané à utiliser.
7. Pour Taux d'initialisation du volume, entrez un taux de 100 — 300 MiB/s. La spécification d'un tarif entraîne des frais supplémentaires. Pour utiliser le taux d'initialisation par défaut ou la restauration rapide de l'instantané, s'il est activé pour le cliché sélectionné, laissez ce champ vide.

 Note

Pour plus d'informations sur la manière dont le débit et la taille complète des données de capture d'écran affectent le temps d'initialisation, consultez [Comment ça marche](#).
Pour en savoir plus sur la tarification, consultez [Facturation](#).

8. Configurez tous les autres paramètres de volume requis et ajoutez des balises si nécessaire.
9. Choisissez Créer un volume.
10. Dans la grille Volumes, visualisez l'état d'initialisation et la progression du volume.

AWS CLI

Pour créer un de volumes

Utilisez la commande [create-volume](#). L'exemple suivant crée un gp3 volume à partir d'un instantané dans la zone de disponibilité spécifiée avec un taux d'initialisation du volume de 300 MiB/s. Remplacez les exemples de région, de zone de disponibilité et d'ID de snapshot par les valeurs de vos ressources :

```
aws ec2 create-volume \
  --region us-east-1 \
  --availability-zone us-east-1a \
```

```
--volume-type gp3 \  
--snapshot-id snap-0abcdef1234567890 \  
--volume-initialization-rate 300
```

Si vous omettez `--size`, le volume utilise la taille de volume de l'instantané source. Si vous spécifiez `--size`, la valeur doit être égale ou supérieure à la taille du volume de l'instantané source.

PowerShell

Pour créer un de volumes

Utilisez l'applet de commande [New-EC2Volume](#). L'exemple suivant crée un gp3 volume à partir d'un instantané dans la zone de disponibilité spécifiée avec un taux d'initialisation du volume de 300 MiB/s. La commande stocke l'objet de volume renvoyé dans `$volume`. Remplacez les exemples de région, de zone de disponibilité et d'ID de snapshot par les valeurs de vos ressources :

```
$volume = New-EC2Volume `  
-Region us-east-1 `  
-AvailabilityZone us-east-1a `  
-VolumeType gp3 `  
-SnapshotId snap-0abcdef1234567890 `  
-VolumeInitializationRate 300
```

Initialisation du moniteur

La mise à jour des informations d'initialisation du volume peut prendre jusqu'à 5 minutes. Pour obtenir des instructions sur la surveillance de l'initialisation, consultez [Surveiller l'état de l'initialisation du volume Amazon EBS](#).

Utiliser un instantané activé pour une restauration rapide

Si vous créez un volume à partir d'un instantané activé pour la restauration rapide des instantanés, le volume est entièrement initialisé lors de la création et affiche immédiatement toutes ses performances. Pour plus d'informations sur l'utilisation de la restauration rapide des instantanés, consultez [Restauration d'instantané rapide Amazon EBS](#).

Initialiser manuellement les volumes après leur création

Vous pouvez initialiser manuellement un volume Amazon EBS après sa création afin de minimiser l'impact de l'initialisation du volume sur les performances.

Vous pouvez utiliser les procédures suivantes pour initialiser manuellement un volume Amazon EBS après sa création.

Important

Lors de l'initialisation de volumes SSD IOPS provisionnés créés à partir de snapshots, les performances du volume peuvent chuter en dessous de 50 % de leur niveau attendu, ce qui entraîne l'affichage d'un warning état lors de la vérification de l'état des performances. I/O Cette situation est attendue et vous pouvez ignorer l'état warning des volumes Provisioned IOPS SSD lorsque vous les initialisez. Pour de plus amples informations, veuillez consulter [Vérifications de l'état des volumes Amazon EBS](#).

Instances Linux

Pour initialiser un volume créé à partir d'un instantané sur Linux

1. Attachez le volume qui vient d'être restauré à votre instance Linux.
2. Utilisez la commande `lsblk` pour afficher les périphériques de stockage en mode bloc attachés à votre instance.

```
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80  0  30G  0 disk
xvda1 202:1   0   8G  0 disk /
```

Ici, vous pouvez voir que le nouveau volume, `/dev/xvdf`, est attaché, mais pas monté (car aucun chemin n'est répertorié sous la colonne `MOUNTPOINT`).

3. Utilisez les utilitaires `dd` ou `fio` pour lire tous les blocs de l'appareil. La commande `dd` est installée par défaut sur les systèmes Linux, mais la commande `fio` est nettement plus rapide dans la mesure où elle permet les lectures multithreads.

 Note

Cette étape peut prendre de plusieurs minutes à plusieurs heures selon la bande passante de votre instance EC2, les IOPS fournies pour le volume et la taille du volume.

[dd] Le paramètre `if` (fichier en entrée) doit être défini sur le lecteur que vous souhaitez initialiser. Le paramètre `of` (fichier de sortie) doit être défini sur l'appareil virtuel null Linux, `/dev/null`. Le paramètre `bs` définit la taille de bloc de l'opération de lecture. Pour des performances optimales, il doit être défini sur 1 Mo.

 Important

L'utilisation incorrecte de la commande `dd` peut facilement entraîner la destruction des données d'un volume. Veillez à suivre précisément l'exemple de commande ci-dessous. Seul le paramètre `if=/dev/xvdf` varie en fonction du nom de l'appareil que vous lisez.

```
$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] Si la commande `fio` est installée sur votre système, utilisez la commande suivante pour initialiser votre volume. Le paramètre `--filename` (fichier en entrée) doit être défini sur le lecteur que vous souhaitez initialiser.

```
$ sudo fio --filename=/dev/xvdf --rw=read --bs=1M --iodepth=32 --ioengine=libaio --direct=1 --name=volume-initialize
```

Pour installer la commande `fio` sur Amazon Linux, utilisez la commande suivante :

```
sudo yum install -y fio
```

Pour installer la commande `fio` sur Ubuntu, utilisez la commande suivante :

```
sudo apt-get install -y fio
```

Une fois l'opération terminée, un rapport s'affiche au sujet de l'opération de lecture. Votre volume est maintenant prêt à être utilisé. Pour de plus amples informations, veuillez consulter [Mettre un volume Amazon EBS à disposition pour utilisation](#).

instances Windows

Avant d'utiliser un outil, rassemblez des informations au sujet des disques sur votre système comme suit :

Pour collecter des informations sur les disques système

1. Utilisez la commande `wmic` afin d'afficher une liste des disques disponibles sur votre système :

```
wmic diskdrive get size,deviceid
```

Voici un exemple de sortie :

DeviceID	Size
\\.\PHYSICALDRIVE2	80517265920
\\.\PHYSICALDRIVE1	80517265920
\\.\PHYSICALDRIVE0	128849011200
\\.\PHYSICALDRIVE3	107372805120

2. Identifiez le disque à initialiser à l'aide de `dd` ou de `fio`. Le lecteur C : se trouve sur `\\.\PHYSICALDRIVE0`. Vous pouvez utiliser l'utilitaire `diskmgmt.msc` afin de comparer les lettres de lecteur aux numéros de lecteur de disque si vous avez des doutes sur le numéro de lecteur à utiliser.

Use the dd utility

Suivez les procédures suivantes pour installer et utiliser `dd` pour initialiser un volume.

Considérations Importantes

- L'initialisation d'un volume peut prendre quelques minutes à plusieurs heures selon la bande passante de votre instance EC2, les IOPS provisionnés pour le volume et la taille du volume.
- L'utilisation incorrecte de la commande `dd` peut facilement entraîner la destruction des données d'un volume. Assurez-vous de suivre précisément cette procédure.

Pour installer dd pour Windows

La commande dd pour le programme Windows fonctionne de la même manière que pour le programme dd généralement disponible pour Linux et les systèmes Unix. Elle vous permet en outre d'initialiser les volumes Amazon EBS qui ont été créés à partir d'instantanés. Les versions bêta les plus récentes prennent en charge le périphérique `/dev/null` virtuel. Si vous installez une version antérieure, vous pouvez utiliser le périphérique `null` virtuel à la place. La documentation complète est disponible à l'adresse <http://www.chrysocome.net/dd>.

1. Téléchargez la version binaire la plus récente de dd pour Windows à l'adresse <http://www.chrysocome.net/dd>.
2. (Facultatif) Créez un dossier pour les utilitaires de ligne de commande en veillant à ce qu'il soit facile à trouver et à mémoriser, par exemple `C:\bin`. Si vous avez déjà un dossier désigné pour les utilitaires de ligne de commande, vous pouvez l'utiliser au cours de l'étape suivante.
3. Décompressez le package binaire et copiez le fichier `dd.exe` dans votre dossier des utilitaires de ligne de commande (par exemple, `C:\bin`).
4. Ajoutez le dossier des utilitaires de ligne de commande à la variable d'environnement Path afin de pouvoir exécuter les programmes de ce dossier où que vous vous trouviez.
 - a. Choisissez Démarrer, ouvrez le menu contextuel (clic droit) pour Ordinateur, puis sélectionnez Propriétés.
 - b. Choisissez Paramètres système avancés, Variables d'environnement.
 - c. Pour Variables système, sélectionnez la variable Chemin et choisissez Modifier.
 - d. Pour Valeur de la variable, ajoutez un point-virgule et l'emplacement de votre dossier des utilitaires de ligne de commande (**`;C:\bin\`**) à la fin de la valeur existante.
 - e. Choisissez OK pour fermer la fenêtre Modifier la variable système.
5. Ouvrez une nouvelle fenêtre d'invite de commandes. L'étape précédente ne met pas à jour les variables d'environnement dans votre fenêtre active d'invite de commandes. Les fenêtres d'invite de commandes que vous ouvrez maintenant que vous avez terminé l'étape précédente sont mises à jour.

Pour initialiser un volume à l'aide de la commande dd pour Windows

Exécutez la commande suivante pour lire tous les blocs sur l'appareil spécifié (et envoyer la sortie vers l'appareil virtuel `/dev/null`). Cette commande initialise en toute sécurité les données existantes.

```
dd if=\\.\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```

Une erreur peut s'afficher si `dd` tente de lire au-delà de la fin du volume. Vous pouvez l'ignorer sans risque.

Si vous avez utilisé une version antérieure de la commande `dd`, celle-ci ne prend pas en charge l'appareil `/dev/null`. Au lieu de cela, vous pouvez utiliser l'appareil `nul` comme suit.

```
dd if=\\.\PHYSICALDRIVEn of=nul bs=1M --progress --size
```

Use the fio utility

Suivez les procédures suivantes pour installer et utiliser `fio` pour initialiser un volume.

Pour installer fio pour Windows

La commande `fio` pour le programme Windows fonctionne de la même manière que pour le programme `fio` généralement disponible pour Linux et les systèmes Unix. Elle vous permet en outre d'initialiser les volumes Amazon EBS qui ont été créés à partir d'instantanés. Pour de plus amples informations, veuillez consulter <https://github.com/axboe/fio>.

1. Téléchargez le programme d'installation [fio MSI](#) en développant Ressources pour la dernière version et en sélectionnant le programme d'installation MSI.
2. Installer `fio`.

Pour initialiser un volume à l'aide de fio pour Windows

1. Exécutez une commande similaire à ce qui suit afin d'initialiser un volume :

```
fio --filename=\\.\PHYSICALDRIVEn --rw=read --bs=1M --iodepth=32 --direct=1 --name=volume-initialize
```

2. Une fois l'opération terminée, vous êtes prêt à utiliser votre nouveau volume. Pour de plus amples informations, veuillez consulter [Mettre un volume Amazon EBS à disposition pour utilisation](#).

Surveiller l'état de l'initialisation du volume Amazon EBS

Lorsque vous créez un volume, à partir d'un instantané ou d'un autre volume (copie du volume), vous pouvez surveiller l'état de l'initialisation du volume pour déterminer si le processus d'initialisation est terminé. Vous pouvez contrôler l'initialisation du volume à l'aide des options suivantes :

Rubriques

- [AWS CLI, AWS Outils pour PowerShell et console Amazon EC2](#)
- [Amazon EventBridge](#)

AWS CLI, AWS Outils pour PowerShell et console Amazon EC2

Vous pouvez utiliser AWS CLI les AWS outils pour PowerShell et la console Amazon EC2 pour vérifier l'état de l'initialisation du volume à tout moment après sa création. Les informations suivantes sont fournies :

- Type d'initialisation (AWS CLI et AWS outils pour PowerShell uniquement) : indique le type d'initialisation du volume utilisé. `default` pour la restauration rapide des instantanés et l'initialisation des volumes par défaut, `provisioned-rate` pour Amazon EBS Provisioned Rate pour l'initialisation des volumes et `volume-copy` pour l'initialisation de la copie des volumes.
- Temps de réalisation estimé (AWS CLI et AWS outils PowerShell uniquement) : uniquement pour les volumes créés à l'aide d'un tarif provisionné Amazon EBS pour l'initialisation des volumes. Temps restant estimé, en secondes, pour terminer l'initialisation du volume.
- Progression : progression, en pourcentage (0 à 100), du processus d'initialisation du volume. Pour les volumes initialisés avec restauration rapide des instantanés, la progression passe à 100 % immédiatement après leur création.
- État d'initialisation : état général de l'initialisation du volume (`initializing` ou `completed`). Pour les volumes initialisés à l'aide de la restauration rapide des instantanés, l'état passe à `completed` immédiatement après leur création.

Note

La mise à jour des informations d'initialisation du volume peut prendre jusqu'à 5 minutes.

Utilisez les onglets suivants pour vérifier l'état d'initialisation du volume.

Console

Pour surveiller l'état de l'initialisation du volume

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume dont vous souhaitez vérifier l'état d'initialisation.
4. Le champ État d'initialisation de la grille et l'onglet Détails fournissent des informations de progression au format suivant : État d'initialisation (pourcentage de progression). Par exemple, Initialisation (75 %).

Les états d'initialisation possibles sont les suivants : Initialisation et Terminé.

AWS CLI

Pour surveiller l'état de l'initialisation du volume

Utilisez la [AWS CLI commande](#) `describe-volume-status` pour afficher l'état de l'initialisation. La sortie inclut `EstimatedTimeToCompleteInSeconds` uniquement les volumes créés avec un tarif provisionné Amazon EBS pour l'initialisation des volumes.

Par exemple, la commande suivante vérifie l'état d'initialisation du volume `vol-11111111111111111`, qui a été créé avec un tarif provisionné Amazon EBS pour l'initialisation du volume.

```
aws ec2 describe-volume-status --volume-ids vol-11111111111111111
```

Voici un exemple de sortie.

```
{
  "VolumeStatuses": [
    {
      "Actions": [],
      "AvailabilityZone": "us-east-1a",
      "Events": [],
      "VolumeId": "vol-11111111111111111",
      "VolumeStatus": {
        "Details": [
          {
```

```

        "Name": "io-enabled",
        "Status": "passed"
      },
      {
        "Name": "io-performance",
        "Status": "not-applicable"
      },
      {
        "Name": "initialization-state",
        "Status": "completed"
      }
    ],
    "Status": "ok"
  },
  "InitializationStatusDetails": {
    "InitializationType": "provisioned-rate",
    "Progress": 75,
    "EstimatedTimeToCompleteInSeconds": 850
  }
}
]
}

```

PowerShell

Pour surveiller l'état de l'initialisation du volume

Utilisez l'[Get-EC2VolumeStatus](#) applet de commande pour afficher l'état de l'initialisation. La sortie inclut `EstimatedTimeToCompleteInSeconds` uniquement les volumes créés avec un tarif provisionné Amazon EBS pour l'initialisation des volumes.

Par exemple, la commande suivante vérifie l'état d'initialisation du volume `vol-11111111111111111`, qui a été créé avec un tarif provisionné Amazon EBS pour l'initialisation du volume.

```

(Get-EC2VolumeStatus `
  -Region us-east-1 `
  -VolumeId vol-11111111111111111).InitializationStatusDetails |
Select-Object `
  InitializationType,
  Progress,
  EstimatedTimeToCompleteInSeconds

```

Amazon EventBridge

Un EventBridge événement Amazon est envoyé à votre compte dans les cinq minutes suivant la fin de l'initialisation du volume. Vous pouvez créer des règles qui déclenchent des actions programmatiques en réponse à ces événements.

Note

- Les événements sont générés dans la mesure du possible.
- Si vous supprimez le volume avant la fin de l'initialisation, ou dans les 5 minutes suivant la fin de l'initialisation, il est possible que vous ne receviez pas l'événement.

Pour plus d'informations sur l'événement, consultez [Événement d'initialisation du volume EBS](#).

Pour surveiller l'état de l'initialisation du volume à l'aide de EventBridge

1. Ouvrez la EventBridge console Amazon à l'adresse <https://console.aws.amazon.com/events/>.
2. Choisissez Règles, puis Créer une règle.
3. Pour l'étape 1, procédez comme suit :
 - a. Spécifiez le nom et la description de la règle.
 - b. Pour Event bus, choisissez le bus qui accueillera les événements. Si vous n'avez pas créé de bus d'événements personnalisé, conservez la valeur par défaut ou consultez [Création d'un bus d'événements](#).
 - c. Pour Type de règle, conservez Règle avec un modèle d'événement.
 - d. Choisissez Suivant.
4. Pour l'étape 2, procédez comme suit :
 - a. Pour Source d'événements, conservez les AWS événements ou les événements des EventBridge partenaires.
 - b. Dans Méthode de création, choisissez Modèle personnalisé (éditeur JSON).
 - c. Pour Modèle d'événement, ajoutez ce qui suit :

```
{  
  "detail-type": ["EBS Volume Notification"],  
  "source": ["aws.ec2"],
```

```
"detail": {  
  "event": ["initializeVolume"],  
  "result": ["succeeded"]  
}
```

Pour voir un exemple d'événement, consultez la section [Événement d'initialisation du volume EBS](#).

- d. Choisissez Suivant.
5. Pour l'étape 3, procédez comme suit :
 - a. Pour Types de cibles, choisissez service AWS .
 - b. Pour Sélectionner la cible, choisissez la rubrique SNS, et pour la rubrique, sélectionnez la rubrique requise. Si vous n'avez créé aucun sujet, consultez la section [Création d'un sujet](#).
 - c. Pour Autorisations, maintenez l'option Utiliser le rôle d'exécution (recommandé) sélectionnée.
 - d. Pour Rôle d'exécution, maintenez l'option Créer un nouveau rôle pour cette ressource spécifique sélectionnée et le nom du rôle par défaut.
 - e. Choisissez Suivant.
6. Pour l'étape 4, spécifiez les balises de la règle si nécessaire, puis choisissez Suivant.
7. Pour l'étape 5, passez en revue la règle, puis choisissez Créer une règle.

Pondération configurable de la bande passante des instances

La configuration de la bande passante d'instance (IBC) est une fonctionnalité qui vous permet d'ajuster l'allocation de bande passante réseau entre Amazon EBS et le réseau VPC pour une instance Amazon EC2. Cette fonctionnalité peut vous aider à optimiser les performances des charges de travail ayant des exigences de bande passante spécifiques. La configuration de la bande passante d'instance n'est prise en charge que sur certaines instances. Pour plus d'informations, consultez Configuration [de la pondération de la bande passante des](#) instances.

Pour les performances EBS, l'utilisation de la pondération de la ebs - 1 bande passante augmente la bande passante EBS de référence de 25 % tout en réduisant la bande passante réseau VPC du même montant absolu. Cela peut être bénéfique pour les I/O-intensive charges de travail nécessitant un débit EBS plus élevé.

Lorsque vous planifiez votre charge de travail, examinez attentivement votre I/O taille et vos modèles. Les I/O tailles plus petites sont généralement moins affectées par les limites de bande passante, tandis que les I/O tailles plus importantes ou les charges de travail séquentielles peuvent subir des impacts plus importants en raison des modifications de bande passante. Il est essentiel de tester minutieusement votre charge de travail spécifique pour garantir des performances optimales avec la pondération de bande passante que vous avez choisie.

Considérations

- La bande passante d'instance configurable est prise en charge sur certains types d'instances. Pour plus d'informations, consultez la section Types d'instances [pris en charge](#).
- L'utilisation de la pondération de la ebs-1 bande passante augmente la bande passante EBS jusqu'à 25 %, ce qui peut améliorer les performances des I/O-intensive applications. Cependant, gardez à l'esprit que la bande passante du réseau VPC sera réduite du même montant absolu (la spécification de bande passante combinée entre EBS et la mise en réseau ne change pas).
- Les modifications de la pondération de la bande passante peuvent affecter de manière significative les I/O performances. Avec la pondération de la vpc-1 bande passante, la bande passante réseau est augmentée, mais il se peut que vous obteniez des IOPS inférieures aux attentes pour les volumes EBS. En effet, il est possible que vous atteigniez la limite de bande passante EBS avant la limite IOPS, en particulier avec des tailles plus importantes I/O . Par exemple, un type d'instance qui prend généralement en charge 240 000 IOPS avec une I/O taille de 16 Ko peut obtenir moins d'IOPS en utilisant le poids de la vpc-1 bande passante en raison de la diminution de la bande passante EBS.
- Testez toujours votre charge de travail spécifique pour vous assurer que la pondération de bande passante que vous avez choisie répond à vos besoins en matière de performances.
- Vous pouvez configurer la pondération de la bande passante lors du lancement de l'instance ou la modifier pour les instances arrêtées. Pour plus d'informations, voir [Configurer la pondération de la bande passante pour votre instance](#).
- Vous pouvez configurer la pondération de la bande passante des instances sans frais supplémentaires.

I/O Caractéristiques et surveillance d'Amazon EBS

Sur une configuration de volume donnée, certaines I/O caractéristiques déterminent le comportement en matière de performances de vos volumes EBS.

- SSD-backed les volumes, le SSD à usage général (gp2etgp3) et le SSD IOPS provisionné (io1etio2), offrent des performances constantes, qu'une I/O opération soit aléatoire ou séquentielle.
- HDD-backed les volumes, le disque dur à débit optimisé (st1) et le disque dur froid (sc1), offrent des performances optimales uniquement lorsque les I/O opérations sont volumineuses et séquentielles.

Pour comprendre comment les volumes SSD et HDD fonctionneront dans votre application, il est important de connaître le lien entre la demande sur le volume, la quantité d'IOPS disponible, le temps nécessaire à l'exécution d'une I/O opération et les limites de débit du volume.

Rubriques

- [IOPS](#)
- [Latence et longueur de file d'attente d'un volume](#)
- [I/O limites de débit en termes de taille et de volume](#)
- [Surveillez les I/O caractéristiques à l'aide CloudWatch](#)
- [Surveillez les statistiques de I/O performance en temps réel](#)
- [Ressources connexes](#)

IOPS

Les IOPS sont une unité de mesure représentant les input/output opérations par seconde. Les opérations sont mesurées en KiB et la technologie de disque sous-jacente détermine la quantité maximale de données qu'un type de volume compte comme un seul I/O. I/O la taille est plafonnée à 256 Ko pour les volumes SSD et à 1 024 Ko pour les volumes de disque dur, car les volumes SSD gèrent les volumes petits ou aléatoires I/O beaucoup plus efficacement que les volumes de disque dur.

Lorsque de petites I/O opérations sont physiquement séquentielles, Amazon EBS tente de les fusionner en une seule I/O opération jusqu'à la taille maximale I/O . De même, lorsque les I/O opérations dépassent la I/O taille maximale, Amazon EBS tente de les diviser en I/O opérations plus petites. Le tableau suivant montre quelques exemples.

Type de volume	I/O Taille maximale	I/O opérations depuis votre application	Nombre d'IOPS	Remarques
SSD	256 Kio	I/O Fonctionnement 1 x 1024 KiB	4 ($1\,024 \div 256 = 4$)	Amazon EBS divise l'opération de 1 024 KiB en quatre I/O opérations plus petites de 256 KiB.
		8 opérations séquentielles de 32 KiB I/O	1 ($8 \times 32 = 256$)	Amazon EBS fusionne les huit I/O opérations séquentielles de 32 KiB en une seule opération de 256 KiB.
		8 I/O opérations aléatoires de 32 Kio	8	Amazon EBS comptabilise les I/O opérations aléatoires séparément.
HDD	1 024 KiB	I/O Fonctionnement 1 x 1024 KiB	1	L' I/O opération est déjà égale à la I/O taille maximale. Elle n'est ni fusionnée ni divisée.
		8 opérations séquentielles de 128 KiB I/O	1 ($8 \times 128 = 1\,024$)	Amazon EBS fusionne les huit opérations séquentielles de 128 KiB en une

Type de volume	I/O Taille maximale	I/O opérations depuis votre application	Nombre d'IOPS	Remarques
				seule I/O opération de 1 024 KiB. I/O
		8 I/O opérations aléatoires de 32 Kio	8	Amazon EBS comptabilise les I/O opérations aléatoires séparément.

Par conséquent, lorsque vous créez un SSD-backed volume supportant 3 000 IOPS (soit en provisionnant un `io1` `io2` volume de 3 000 IOPS, soit en dimensionnant un `gp2` volume à 1 000 GiB, soit en utilisant un `gp3` volume) et que vous l'associez à une EBS-optimized instance capable de fournir une bande passante suffisante, vous pouvez transférer jusqu'à 3 000 I/Os données par seconde, le débit étant déterminé par la taille. I/O

Latence et longueur de file d'attente d'un volume

La longueur de la file d'attente des volumes est le nombre de I/O demandes en attente pour un appareil. La latence est le temps client réel de bout en bout d'une I/O opération, c'est-à-dire le temps écoulé entre l'envoi d'un message I/O à EBS et la réception d'un accusé de réception de la part d'EBS indiquant que la I/O lecture ou l'écriture est terminée. La longueur de la file d'attente doit être correctement calibrée en fonction de I/O la taille et de la latence pour éviter de créer des goulots d'étranglement sur le système d'exploitation client ou sur la liaison réseau vers EBS.

La longueur de la file d'attente optimale varie en fonction des charges de travail, selon la sensibilité de votre application à la latence et à l'IOPS. Si votre charge de travail ne fournit pas suffisamment de I/O demandes pour utiliser pleinement les performances disponibles pour votre volume EBS, il est possible que votre volume ne fournisse pas les IOPS ou le débit que vous avez provisionnés.

Transaction-intensive les applications sont sensibles à l'augmentation de I/O la latence et sont bien adaptées aux SSD-backed volumes. Vous pouvez conserver des IOPS élevées et une latence faible grâce à une longueur de file d'attente moyenne réduite et à un nombre élevé d'IOPS disponibles pour le volume. L'augmentation constante d'un nombre d'IOPS supérieur à celui disponible sur un volume peut entraîner une augmentation de la I/O latence. Pour une cohérence maximale, un volume doit

maintenir une profondeur de file d'attente moyenne (arrondie au nombre entier le plus proche) de 1 pour 1 000 IOPS provisionnées en une minute. Par exemple, pour un volume provisionné avec 3 000 IOPS, la profondeur moyenne de la file d'attente doit être de 3.

Throughput-intensive les applications sont moins sensibles à l'augmentation de la I/O latence et sont bien adaptées aux HDD-backed volumes. Vous pouvez maintenir un débit élevé pour les HDD-backed volumes en maintenant une longueur de file d'attente élevée lorsque vous effectuez des opérations séquentielles volumineuses I/O.

I/O limites de débit en termes de taille et de volume

En ce qui concerne les SSD-backed volumes, si votre I/O taille est très importante, le nombre d'IOPS peut être inférieur à celui que vous avez provisionné, car vous atteignez la limite de débit du volume. Par exemple, un gp2 volume inférieur à 1 000 GiB avec des crédits de rafale disponibles a une limite d'IOPS de 3 000 et une limite de débit de 250. MiB/s Si vous utilisez une I/O taille de 256 KiB, votre volume atteint sa limite de débit à 1 000 IOPS ($1\,000 \times 256\text{ KiB} = 250\text{ MiB}$). Pour les plus petites I/O tailles (telles que 16 KiB), ce même volume peut supporter 3 000 IOPS car le débit est bien inférieur à 250 MiB/s. (Ces exemples supposent que le volume I/O n'atteint pas les limites de débit de l'instance.) Pour plus d'informations sur les limites de débit pour chaque type de volume EBS, consultez [Types de volume Amazon EBS](#).

Pour les petites I/O opérations, vous pouvez constater une valeur IOPS supérieure à celle provisionnée, mesurée depuis l'intérieur de votre instance. Cela se produit lorsque le système d'exploitation de l'instance fusionne de petites I/O opérations en une opération plus importante avant de les transmettre à Amazon EBS.

Si votre charge de travail utilise des entrées HDD-backed st1 et I/Os des sc1 volumes séquentiels, vous risquez de rencontrer un nombre d'IOPS plus élevé que prévu, mesuré depuis l'intérieur de votre instance. Cela se produit lorsque le système d'exploitation de l'instance fusionne les données séquentielles I/Os et les compte en 1 KiB-sized 024 unités. Si votre charge de travail est faible ou aléatoire I/Os, il se peut que le débit soit inférieur à ce que vous attendiez. En effet, chaque opération aléatoire et non séquentielle est prise en I/O compte dans le nombre total d'IOPS, ce qui peut vous faire atteindre la limite d'IOPS du volume plus tôt que prévu.

Quel que soit le type de volume EBS, si vous n'obtenez pas les IOPS ou le débit que vous attendez dans votre configuration, assurez-vous que la bande passante de votre instance EC2 n'est pas le facteur limitant. Vous devez toujours utiliser une instance de génération actuelle (ou une EBS-optimized instance qui inclut 10 connexions Gb/s réseau) pour des performances optimales.

Une autre raison possible pour laquelle vous n'obtenez pas les IOPS attendues est que vous ne conduisez pas suffisamment I/O vers les volumes EBS.

Surveillez les I/O caractéristiques à l'aide CloudWatch

Vous pouvez surveiller ces I/O caractéristiques à l'aide des mesures de [CloudWatch volume de chaque volume](#).

Moniteur pour les personnes bloquées I/O

VolumeStalledIOCheck surveille le statut de vos volumes EBS afin de déterminer à quel moment ils sont dégradés. La métrique est une valeur binaire qui renvoie un statut 0 (réussite) ou 1 (échec) selon que le volume EBS peut effectuer des I/O opérations ou non.

Si la VolumeStalledIOCheck métrique échoue, vous pouvez soit AWS attendre que le problème soit résolu, soit prendre des mesures, telles que remplacer le volume concerné ou arrêter et redémarrer l'instance à laquelle le volume est attaché. Dans la plupart des cas, lorsque cette métrique échoue, EBS diagnostique et restaure automatiquement votre volume en quelques minutes. Vous pouvez utiliser l' [I/Oaction](#) Pause AWS Fault Injection Service pour exécuter des expériences contrôlées afin de tester votre architecture et votre surveillance en fonction de cette métrique afin d'améliorer votre résilience aux défaillances de stockage.

Surveiller I/O la latence d'un volume

Vous pouvez surveiller la latence moyenne des opérations de lecture et d'écriture pour un volume Amazon EBS à l'aide des VolumeAvgWriteLatency métriques VolumeAvgReadLatency et, respectivement. Vous pouvez utiliser l'[action d'injection de](#) latence AWS Fault Injection Service pour exécuter des expériences contrôlées afin de tester votre architecture et votre surveillance sur la base de cette métrique afin d'améliorer votre résilience face à la dégradation des performances de stockage.

Si votre I/O latence est supérieure à ce dont vous avez besoin, assurez-vous que votre application n'essaie pas de générer plus d'IOPS ou de débit que ce que vous avez configuré pour votre volume. Vous pouvez utiliser les VolumeAvgThroughput métriques VolumeAvgIOPS et pour surveiller la moyenne des IOPS et du débit acheminés vers votre volume en une minute, puis les comparer aux IOPS et au débit provisionnés du volume. Si le volume n'entraîne aucune opération pendant la minute, les métriques indiqueront une valeur de zéro (0). Si des rafales d'IOPS ou de débit élevés se produisent pendant une durée inférieure à l'intervalle d'une minute, le volume subit des micro-rafales, mais les mesures moyennes d'IOPS et de débit peuvent indiquer que vous générez des

performances inférieures aux limites d'IOPS ou de débit provisionnées de votre volume. Pour déterminer si votre volume connaît des pics de performances au cours d'une minute donnée, vous pouvez utiliser les `VolumeThroughputExceededCheck` indicateurs `VolumeIOPSExceededCheck` et. Vous pouvez surveiller ces indicateurs pour déterminer si votre charge de travail a constamment tenté de générer des IOPS ou un débit supérieur aux performances provisionnées de votre volume au cours d'une minute donnée. Si les IOPS pilotées pendant une seconde au cours de la minute dépassent systématiquement les performances IOPS provisionnées de votre volume, la `VolumeIOPSExceededCheck` métrique est renvoyée. 1 Si le débit piloté pendant une seconde au cours de la minute dépasse régulièrement les performances de débit provisionnées de votre volume, la `VolumeThroughputExceededCheck` métrique est 1 renvoyée. Si les IOPS et le débit pilotés se situent dans les limites des performances provisionnées de votre volume, les mesures sont renvoyées. 0

Si votre application a besoin d'un nombre d'IOPS supérieur à ce que votre volume peut fournir, envisagez d'utiliser l'une des options suivantes :

- Un volume gp3, io2, ou io1 approvisionné avec suffisamment d'IOPS pour atteindre la latence requise
- Un volume gp2 plus important qui fournit des performances IOPS de base suffisantes

HDD-backed st1 et les sc1 volumes sont conçus pour fonctionner au mieux avec des charges de travail qui tirent parti de la taille maximale I/O de 1 024 Ko. Pour déterminer la I/O taille moyenne de votre volume, divisez `VolumeWriteBytes` par `VolumeWriteOps`. Le même calcul s'applique pour les opérations de lecture. Si I/O la taille moyenne est inférieure à 64 Ko, l'augmentation de la taille I/O des opérations envoyées vers un sc1 volume st1 ou devrait améliorer les performances.

Surveillez l'équilibre des compartiments en rafale pour les **volumes gp2, st1 et sc1**

`BurstBalance` affiche l'équilibre du compartiment en rafales des volumes gp2, st1 et sc1 sous forme de pourcentage du solde restant. Lorsque votre compartiment de rafale est épuisé, le volume I/O (pour les gp2 volumes) ou le débit volumique (pour st1 et les sc1 volumes) est limité au niveau de référence. Vérifiez la valeur `BurstBalance` pour déterminer si votre volume est limité pour cette raison. Pour obtenir la liste complète des métriques Amazon EBS disponibles, consultez [Statistiques CloudWatch Amazon pour Amazon EBS](#) la section Statistiques [Amazon EBS pour Nitro-based les instances](#).

Surveillez les statistiques de I/O performance en temps réel

Vous pouvez accéder à des statistiques de performances détaillées en temps réel pour les volumes Amazon EBS attachés aux instances Nitro-based Amazon EC2.

Vous pouvez combiner ces statistiques pour calculer la latence moyenne et les IOPS, ou pour vérifier si les I/O opérations sont terminées. Vous pouvez également consulter la durée totale pendant laquelle votre application a dépassé les limites d'IOPS ou de débit provisionnées de votre volume EBS ou de l'instance attachée. En suivant l'évolution de ces statistiques au fil du temps, vous pouvez déterminer si vous devez augmenter vos IOPS provisionnées ou vos limites de débit pour optimiser les performances de votre application. Les statistiques de performances détaillées incluent également des histogrammes pour les I/O opérations de lecture et d'écriture, qui fournissent une distribution de votre I/O latence en gardant une trace du nombre total d' I/O opérations effectuées dans une bande de latence.

Pour de plus amples informations, veuillez consulter [Statistiques de performances détaillées d'Amazon EBS](#).

Ressources connexes

Pour plus d'informations sur les I/O caractéristiques d'Amazon EBS, consultez la présentation re:Invent suivante : [Amazon EBS : Designing for Performance](#).

Configuration Amazon EBS et RAID

Avec Amazon EBS, vous pouvez utiliser toute configuration RAID standard que vous pourriez utiliser avec un serveur bare metal traditionnel, dans la mesure où cette configuration RAID est prise en charge par le système d'exploitation de votre instance. Cela est dû au fait que l'ensemble de la configuration RAID est mise en œuvre au niveau logiciel.

Les données de volume Amazon EBS sont répliquées sur plusieurs serveurs dans une zone de disponibilité pour éviter la perte de données résultant de la défaillance d'un seul composant. Cette réplication rend les volumes Amazon EBS dix fois plus fiables que les disques durs classiques.

Pour plus d'informations, consultez la section Fonctionnalités <https://aws.amazon.com/ebs/features/> d'Amazon EBS.

Table des matières

- [Options de configuration RAID](#)
- [Création d'une matrice RAID 0](#)

- [Créer des instantanés de volumes dans une grappe RAID](#)

Options de configuration RAID

La création d'une grappe RAID 0 vous permet d'obtenir un niveau de performance plus élevé pour un système de fichiers que vous pouvez mettre en service sur un volume Amazon EBS unique. Utilisez RAID 0 lorsque I/O les performances sont de la plus haute importance. Avec RAID 0, I/O il est distribué sur les volumes en une bande. Si vous ajoutez un volume, du débit et des IOPS sont ajoutés directement. Cependant, gardez à l'esprit que les performances de l'agrégat par bandes sont limitées à celles du volume le moins performant, et que la perte d'un seul volume entraîne la perte complète des données pour la grappe.

La taille résultante d'une grappe RAID 0 est la somme des tailles des volumes contenues par celle-ci, et la bande passante correspond au total de bande passante disponible des volumes de la grappe. Par exemple, deux `io1` volumes de 500 GiB avec 4 000 IOPS provisionnées chacun créent une matrice RAID 0 de 1 000 GiB avec une bande passante disponible de 8 000 IOPS et 1 000 de débit. MiB/s

Important

RAID 5 et RAID 6 ne sont pas recommandés pour Amazon EBS, car les opérations d'écritures de parité de ces modes RAID consomment certaines des IOPS (IOPS) disponibles pour vos volumes. En fonction de la configuration de votre grappe RAID, ces modes RAID fournissent de 20 à 30 % d'IOPS utilisables en moins qu'une configuration RAID 0. Le coût accru est également un facteur à prendre en compte avec ces modes RAID ; avec l'utilisation de tailles et de vitesses de volume identiques, une grappe RAID 0 à 2 volumes peut offrir de meilleures performances qu'une grappe RAID 6 à 4 volumes dont le coût est deux fois plus élevé.

L'utilisation d'un RAID 1 n'est pas non plus recommandée avec Amazon EBS. Un RAID 1 nécessite une plus grande bande passante entre Amazon EC2 et Amazon EBS que les configurations non-RAID, car les données sont écrites simultanément sur plusieurs volumes. En outre, un RAID 1 ne fournit aucune amélioration des performances d'écriture.

Création d'une matrice RAID 0

Pour créer la grappe RAID 0, suivez la procédure suivante.

Considérations

- Avant d'exécuter cette procédure, vous devez décider de la taille de votre matrice RAID 0 et du nombre d'IOPS à provisionner.
- Créez des volumes avec des tailles et des valeurs de performances d'IOPS (IOPS) identiques pour votre grappe. Veillez à ne pas créer une grappe qui dépasse la bande passante disponible de votre instance EC2.
- Vous devez éviter de démarrer à partir d'un volume RAID. Si l'un des périphériques tombe en panne, il est possible que vous ne puissiez pas démarrer le système d'exploitation.

Instances Linux

Pour créer une grappe RAID 0 sous Linux

1. Créez les volumes Amazon EBS pour votre grappe. Pour de plus amples informations, veuillez consulter [Créez un volume Amazon EBS](#).
2. Attachez les volumes Amazon EBS à l'instance devant héberger la grappe. Pour plus d'informations, consultez [Attacher un volume Amazon EBS à une instance Amazon EC2](#).
3. Utilisez la commande mdadm pour créer une unité RAID logique à partir des volumes Amazon EBS nouvellement attachés. Remplacez le nombre de volumes de votre baie par *number_of_volumes* et les noms de périphériques de chaque volume de la baie (par exemple /dev/xvdf) par *device_name*. Vous pouvez également *MY_RAID* remplacer le tableau par votre propre nom unique.

Note

Vous pouvez afficher la liste des unités de votre instance avec la commande lsblk pour trouver les noms d'unité.

Pour créer une grappe RAID 0, exécutez la commande suivante (notez l'option `--level=0` pour agréger la grappe) :

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --  
raid-devices=number_of_volumes device_name1 device_name2
```

 Tip

Si l'erreur `mdadm: command not found` s'affiche, utilisez la commande suivante pour installer `mdadm` : `sudo yum install mdadm`.

4. Laissez à la grappe RAID le temps de s'initialiser et se synchroniser. Vous pouvez suivre la progression de ces opérations avec la commande suivante :

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

Voici un exemple de sortie :

```
Personalities : [raid0]
md0 : active raid0 xvd1[1] xvd1[0]
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

En général, vous pouvez afficher des informations détaillées sur votre grappe RAID avec la commande suivante :

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

Voici un exemple de sortie :

```
/dev/md0:
      Version : 1.2
  Creation Time : Wed May 19 11:12:56 2021
    Raid Level : raid0
    Array Size : 41910272 (39.97 GiB 42.92 GB)
   Raid Devices : 2
  Total Devices : 2
 Persistence : Superblock is persistent

   Update Time : Wed May 19 11:12:56 2021
     State : clean
 Active Devices : 2
Working Devices : 2
 Failed Devices : 0
```

Spare Devices : 0

Chunk Size : 512K

Consistency Policy : none

Name : MY_RAID

UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c

Events : 0

Number	Major	Minor	RaidDevice	State	
0	202	16	0	active sync	/dev/sdb
1	202	32	1	active sync	/dev/sdc

5. Créez un système de fichiers sur votre grappe RAID et attribuez-lui une étiquette à utiliser quand vous le monterez ultérieurement. Par exemple, pour créer un système de fichiers ext4 avec l'étiquette **MY_RAID**, exécutez la commande suivante :

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

Selon les exigences de votre application ou les restrictions de votre système d'exploitation, vous pouvez utiliser un autre système de fichiers, comme ext3 ou XFS (consultez la documentation relative à votre système de fichiers pour trouver la commande de création de système de fichiers correspondante).

6. Pour vous assurer que la matrice RAID est réassemblée automatiquement au démarrage, créez un fichier de configuration contenant les informations RAID :

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

Note

Si vous utilisez une distribution Linux autre qu'Amazon Linux, il se peut que vous deviez modifier cette commande. Par exemple, il se peut que vous deviez placer le fichier dans un autre emplacement, ou ajouter le Paramètre `--examine`. Pour plus d'informations, exécutez `man mdadm.conf` sur votre instance Linux.

7. Créez une nouvelle image ramdisk pour précharger correctement les modules de périphérique de stockage en mode bloc pour votre nouvelle configuration RAID :


```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. Créez un point de montage (mount) pour votre grappe RAID.

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. Enfin, montez l'unité RAID sur le point de montage que vous avez créé :

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

Votre unité RAID est maintenant prête à être utilisée.

10. (Facultatif) Pour monter ce volume Amazon EBS à chaque redémarrage du système, ajoutez une entrée pour l'appareil dans le fichier `/etc/fstab`.

- a. Créez une sauvegarde de votre fichier `/etc/fstab` que vous pouvez utiliser si vous détruisez ou supprimez accidentellement ce fichier en l'éditant.

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

- b. Ouvrez le fichier `/etc/fstab` avec votre éditeur de texte préféré (comme nano ou vim).
- c. Placez en commentaires les lignes commençant par « `UUID=` » et, à la fin du fichier, ajoutez une nouvelle ligne pour votre volume RAID à l'aide du format suivant :

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

Les trois derniers champs de cette ligne correspondent aux options de montage du système de fichiers, à la fréquence de vidage du système de fichiers et à l'ordre des contrôles de système de fichiers au démarrage. Si vous ne savez pas quelles valeurs utiliser, utilisez les valeurs de l'exemple ci-dessous (`defaults,nofail 0 2`). Pour plus d'informations sur les entrées `/etc/fstab`, consultez la page du manuel `fstab` (en entrant `man fstab` sur la ligne de commande). Par exemple, pour monter le système de fichiers `ext4` sur l'unité avec l'étiquette `MY_RAID` au point de montage `/mnt/raid`, ajoutez l'entrée suivante à `/etc/fstab`.

 Note

Si jamais vous prévoyez de démarrer votre instance sans ce volume attaché (par exemple, pour que ce volume puisse basculer entre différentes instances), vous devez ajouter l'option de montage `nofail` qui permet à l'instance de démarrer même si des erreurs se produisent lors du montage du volume. Les dérivés Debian, comme Ubuntu, doivent également ajouter l'option de montage `nobootwait`.

```
LABEL=MY_RAID      /mnt/raid  ext4    defaults,nofail    0      2
```

- d. Après avoir ajouté la nouvelle entrée à `/etc/fstab`, vous devez vérifier que celle-ci fonctionne. Exécutez la commande `sudo mount -a` pour monter tous les systèmes de fichiers dans `/etc/fstab`.

```
[ec2-user ~]$ sudo mount -a
```

Si la commande précédente ne génère pas d'erreur, votre fichier `/etc/fstab` est correct et votre système de fichiers sera monté automatiquement au prochain démarrage. Si la commande génère des erreurs, examinez celles-ci et essayez de corriger votre fichier `/etc/fstab`.

 Warning

Des erreurs dans le fichier `/etc/fstab` peuvent rendre un système impossible à démarrer. N'arrêtez pas un système dont le fichier `/etc/fstab` contient des erreurs.

- e. (Facultatif) Si vous n'êtes pas sûr de savoir comment corriger des erreurs dans `/etc/fstab`, vous avez toujours la possibilité de restaurer votre fichier `/etc/fstab` de sauvegarde avec la commande suivante.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

instances Windows

Pour créer une grappe RAID 0 sous Windows

1. Créez les volumes Amazon EBS pour votre grappe. Pour de plus amples informations, veuillez consulter [Créez un volume Amazon EBS..](#)
2. Attachez les volumes Amazon EBS à l'instance devant héberger la grappe. Pour plus d'informations, consultez [Attacher un volume Amazon EBS à une instance Amazon EC2.](#)
3. Connectez-vous à votre instance Windows. Pour plus d'informations, consultez [Connexion à votre instance Windows.](#)
4. Ouvrez une invite de commande et tapez la commande diskpart.

diskpart

```
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51C0
```

5. A l'invite DISKPART, affichez la liste des disques disponibles avec la commande suivante.

```
DISKPART> list disk
```

Disk ###	Status	Size	Free	Dyn	Gpt
-----	-----	-----	-----	---	---
Disk 0	Online	30 GB	0 B		
Disk 1	Online	8 GB	0 B		
Disk 2	Online	8 GB	0 B		

Identifiez les disques que vous souhaitez utiliser dans votre grappe et notez leurs numéros.

6. Chaque disque à utiliser dans votre grappe doit être un disque dynamique en ligne ne contenant pas de volumes existants. Utilisez les étapes suivantes pour convertir des disques de base en disques dynamiques et supprimer les volumes existants.
 - a. Sélectionnez le disque que vous souhaitez utiliser dans votre baie à l'aide de la commande suivante, en le *n* remplaçant par votre numéro de disque.

```
DISKPART> select disk n
```

```
Disk n is now the selected disk.
```

- b. Si le disque sélectionné est affiché comme étant `Offline`, mettez-le en ligne en exécutant la commande `online disk`.
- c. Si le disque sélectionné ne comporte pas d'astérisque dans la colonne `Dyn` dans la sortie de la commande `list disk` précédente, vous devez le convertir en disque dynamique.

```
DISKPART> convert dynamic
```

 Note

Si une erreur indique que le disque est protégé en écriture, vous pouvez effacer l'indicateur de lecture seule avec la commande `ATTRIBUTE DISK CLEAR READONLY`, puis retenter la conversion en disque dynamique.

- d. Utilisez la commande `detail disk` pour vérifier s'il existe des volumes sur le disque sélectionné.

```
DISKPART> detail disk
```

```
XENSRC PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type    : SCSI
Status  : Online
Path    : 0
Target  : 1
LUN ID  : 0
Location Path : PCIR00T(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only   : No
Boot Disk   : No
Pagefile Disk : No
Hibernation File Disk : No
Crashdump Disk : No
Clustered Disk : No
```

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
Volume 2	D	NEW VOLUME	FAT32	Simple	8189 MB	Healthy	

Notez les numéros des volumes figurant sur le disque. Dans cet exemple, le numéro de volume est 2. Si le disque ne contient pas de volume, vous pouvez ignorer l'étape suivante.

- e. (Obligatoire uniquement si des volumes ont été identifiés à l'étape précédente) Sélectionnez et supprimez les volumes existants sur le disque que vous avez identifiés à l'étape précédente.

 Warning

Cette opération détruit les données existant sur le volume.

- i. Sélectionnez le volume en le **n** remplaçant par votre numéro de volume.

```
DISKPART> select volume n
Volume n is the selected volume.
```

- ii. Supprimez le volume.

```
DISKPART> delete volume

DiskPart successfully deleted the volume.
```

- iii. Répétez ces sous-étapes pour chaque volume à supprimer sur le disque sélectionné.

- f. Répétez l'opération [Step 6](#) pour chaque disque à utiliser dans votre grappe.

7. Vérifiez que les disques que vous voulez utiliser sont maintenant dynamiques. Dans ce cas, cet exemple utilise les disques 1 et 2 pour le volume RAID.

```
DISKPART> list disk
```

Disk ###	Status	Size	Free	Dyn	Gpt
-----	-----	-----	-----	---	---
Disk 0	Online	30 GB	0 B		
Disk 1	Online	8 GB	0 B	*	
Disk 2	Online	8 GB	0 B	*	

8. Créez votre grappe RAID. Sous Windows, un volume RAID 0 est appelé volume agrégé par bandes.

Pour créer une grappe de volumes agrégés par bandes sur les disques 1 et 2, utilisez la commande suivante (notez l'option `stripe` pour agréger la grappe) :

```
DISKPART> create volume stripe disk=1,2
```

```
DiskPart successfully created the volume.
```

9. Vérifiez votre nouveau volume.

```
DISKPART> list volume
```

```
DISKPART> list volume
```

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
Volume 0	C		NTFS	Partition	29 GB	Healthy	System
Volume 1			RAW	Stripe	15 GB	Healthy	

Remarquez que la colonne Type indique maintenant que le volume 1 est un volume stripe.

10. Sélectionnez et formatez votre volume pour pouvoir commencer à l'utiliser.

- Sélectionnez le volume que vous souhaitez formater, en le *n* remplaçant par votre numéro de volume.

```
DISKPART> select volume n
```

```
Volume n is the selected volume.
```

- Formatez le volume.

Note

Pour effectuer un formatage complet, omettez l'option quick.

```
DISKPART> format quick recommended label="My new volume"
```

```
100 percent completed
```

```
DiskPart successfully formatted the volume.
```

- Affectez une lettre de lecteur disponible à votre volume.

```
DISKPART> assign letter f
```

```
DiskPart successfully assigned the drive letter or mount point.
```

Votre nouveau volume est maintenant prêt à être utilisé.

Créer des instantanés de volumes dans une grappe RAID

Si vous souhaitez sauvegarder les données des volumes EBS d'une matrice RAID à l'aide de snapshots, vous devez vous assurer que les snapshots sont cohérents. La raison en est que les instantanés de ces volumes sont créés indépendamment. La restauration de volumes EBS d'une grappe RAID à partir d'instantanés non synchronisés peut dégrader l'intégrité de la grappe.

Pour créer un ensemble cohérent d'instantanés pour votre matrice RAID, utilisez les instantanés [multi-volumes EBS](#). Multi-volume les instantanés vous permettent de prendre des instantanés instantanés, coordonnés avec les données et cohérents en cas de panne sur plusieurs volumes EBS attachés à une instance EC2. Il n'est pas nécessaire d'arrêter votre instance pour assurer la coordination entre les volumes afin de garantir la cohérence, car des instantanés sont automatiquement pris sur plusieurs volumes EBS. Pour plus d'informations, consultez les étapes de création d'instantanés multi-volumes sous [Créer des instantanés Amazon EBS](#).

Volumes Amazon EBS de référence

Vous pouvez tester les performances des volumes Amazon EBS en simulant I/O des charges de travail. Procédez comme suit :

1. Lancez une EBS-optimized instance.
2. Créez des volumes EBS.
3. Associez les volumes à votre EBS-optimized instance.
4. Configurez et installez le périphérique de stockage en mode bloc.
5. Installez un outil pour évaluer les I/O performances.
6. Comparez les I/O performances de vos volumes.
7. Supprimez vos volumes et mettez l'instance hors service pour éviter de générer des frais.

 Important

Certaines des procédures entraîneront la destruction des données existantes sur les volumes EBS que vous comparez. Les procédures de comparaison sont conçues pour être utilisées sur des volumes créés spécialement à des fins de tests, et pas sur des volumes de production.

Configurer votre instance

Pour optimiser les performances des volumes EBS, nous vous recommandons d'utiliser une EBS-optimized instance. EBS-optimized les instances fournissent une bande passante dédiée entre Amazon EC2 et Amazon EBS, avec des spécifications en fonction du type d'instance.

Pour créer une EBS-optimized instance, choisissez Lancer en tant qu' EBS-optimizedinstance lorsque vous lancez l'instance à l'aide de la console Amazon EC2, ou spécifiez-la `--ebs-optimized` lorsque vous utilisez la ligne de commande. Assurez-vous de sélectionner un type d'instance qui prend en charge cette option.

Configurer des volumes Provisioned IOPS SSD ou SSD à usage général

Pour créer un SSD à IOPS provisionnés (io1 et io2) ou un SSD à usage général (gp2 et gp3) à l'aide de la console Amazon EC2, pour Volume type (Type de volume), choisissez Provisioned IOPS SSD (io1) (SSD à IOPS provisionnés (io1)), Provisioned IOPS SSD (io2) (SSD à IOPS provisionnés (io2)), General Purpose SSD (gp2) (SSD à usage général (gp2)) ou General Purpose SSD (gp3) (SSD à usage général (gp3)). Sur la ligne de commande, spécifiez io1, io2, gp2 ou gp3 pour le paramètre `--volume-type`. Pour les gp3 volumes io1io2, et, spécifiez le nombre d'I/O opérations par seconde (IOPS) pour le `--iops` paramètre. Pour plus d'informations, consultez [Types de volume Amazon EBS](#) et [Créez un volume Amazon EBS](#).

(Instances Linux uniquement) Pour les exemples de tests, nous vous recommandons de créer une matrice RAID 0 à 6 volumes, qui offre un haut niveau de performances. Dans la mesure où vous êtes facturé en fonction des gigaoctets provisionnés (et du nombre d'IOPS provisionnés pour les volumes io1, io2 et gp3), et non du nombre de volumes, aucun coût supplémentaire ne sera appliqué pour la création de plusieurs volumes de plus petite taille, puis pour leur utilisation afin de créer un agrégat par bandes. Si vous utilisez Oracle Orion afin de comparer vos volumes, vous pouvez effectuer une simulation de l'agrégation par bandes comme avec Oracle ASM. C'est pourquoi nous

vous recommandons de laisser Orion se charger de l'agrégation par bandes. Si vous utilisez un outil de comparaison différent, vous devez effectuer vous-même l'agrégation des volumes par bandes.

Pour plus d'informations sur la création d'une matrice RAID 0, consultez [Création d'une matrice RAID 0](#).

Configurer des volumes de disque dur à débit optimisé (**st1**) ou de disque dur froid (**sc1**)

Pour créer un volume **st1**, choisissez HDD à débit optimisé lorsque vous créez le volume via la console Amazon EC2 ou spécifiez `--type st1` si vous utilisez la ligne de commande. Pour créer un volume **sc1**, choisissez HDD à froid lorsque vous créez le volume via la console Amazon EC2 ou spécifiez `--type sc1` si vous utilisez la ligne de commande. Pour plus d'informations sur la création de volumes EBS, consultez [Créez un volume Amazon EBS](#). Pour plus d'informations sur la liaison de ces volumes à votre instance, consultez [Attacher un volume Amazon EBS à une instance Amazon EC2](#).

(instances Linux uniquement) AWS fournit un modèle JSON à utiliser CloudFormation qui simplifie cette procédure de configuration. Accédez au [modèle](#) et enregistrez-le en tant que fichier JSON. CloudFormation vous permet de configurer vos propres clés SSH et de configurer plus facilement un environnement de test de performance pour évaluer les **st1** volumes. Le modèle crée une instance de la génération actuelle et un volume **st1** de 2 TiO, et attache ce dernier à l'instance dans `/dev/xvdf`.

(Instances Linux uniquement) Pour créer un volume de disque dur à l'aide du modèle

1. Ouvrez la CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Choisissez Create Stack.
3. Choisissez Télécharger un modèle sur Amazon S3 et sélectionnez le modèle JSON que vous avez obtenu précédemment.
4. Attribuez un nom à votre stack (comme "test-perf-efs"), puis sélectionnez un type d'instance (par défaut : r3.8xlarge) et une clé SSH.
5. Choisissez Suivant à deux reprises, puis sélectionnez Créer une pile.
6. Lorsque l'état de votre nouvelle pile passe de CREATE_IN_PROGRESS à COMPLETE, choisissez Outputs (Sorties) afin d'obtenir l'entrée DNS publique de votre nouvelle instance, qui sera attachée à un volume **st1** de 2 TiO.

7. Connectez-vous à votre nouvelle pile via SSH en tant qu'utilisateur **ec2-user**, avec le nom d'hôte obtenu à partir de l'entrée DNS lors de l'étape précédente.
8. Passez à [Installer les outils d'évaluation](#).

Installer les outils d'évaluation

Les tableaux suivants répertorient certains des outils que vous pouvez utiliser pour évaluer les performances des volumes EBS.

Instances Linux

Outil	Description
fio	<p>Pour évaluer les I/O performances. (Notez que la commande fio a une dépendance sur <code>libaio-devel</code>.)</p> <p>Pour installer fio sur Amazon Linux, exécutez la commande suivante :</p> <pre>\$ sudo yum install -y fio</pre> <p>Pour installer fio sur Ubuntu, exécutez la commande suivante :</p> <pre>sudo apt-get install -y fio</pre>
Outil de calibrage Oracle Orion	Pour calibrer les I/O performances des systèmes de stockage à utiliser avec les bases de données Oracle.

instances Windows

Outil	Description
DiskSpd	DiskSpd est un outil de performance de stockage développé par les équipes d'ingénierie d'infrastructure Windows, Windows Server et Cloud Server de Microsoft. Il est disponible en téléchargement à l'adresse https://github.com/Microsoft/diskspd/releases .

Outil	Description
	<p>Après avoir téléchargé le fichier exécutable <code>diskspd.exe</code>, ouvrez une invite de commande avec des droits d'administration (en choisissant « Exécuter en tant qu'administrateur »), puis accédez au répertoire où vous avez copié le fichier <code>diskspd.exe</code>.</p> <p>Copiez le fichier <code>diskspd.exe</code> exécutable souhaité à partir du dossier exécutable approprié (<code>amd64fre</code>, <code>armfre</code> ou <code>x86fre</code>) vers un chemin d'accès court et simple tel que <code>C:\DiskSpd</code>. Dans la plupart des cas, vous aurez besoin de la version 64 bits de DiskSpd from the <code>amd64fre</code> folder.</p> <p>Le code source de DiskSpd est hébergé GitHub sur : https://github.com/Microsoft/diskspd.</p>
CrystalDiskMark	<p>CrystalDiskMark est un simple logiciel de référence de disque. Il est disponible en téléchargement à l'adresse https://crystalmark.info/en/software/crystaldiskmark/.</p>

Ces outils de comparaison prennent en charge un large éventail de paramètres de test. Vous devez utiliser des commandes proches des charges de travail que vos volumes devront prendre en charge. Les commandes ci-dessous sont proposées à titre d'exemple pour vous permettre de débiter.

Choisir la longueur de la file d'attente d'un volume

Choisissez la meilleure longueur de file d'attente du volume en fonction de votre charge de travail et du type de volume.

Longueur de la file d'attente pour les SSD-backed volumes

Pour déterminer la longueur de file d'attente optimale pour votre charge de travail sur les SSD-backed volumes, nous vous recommandons de cibler une longueur de file d'attente de 1 pour 1 000 IOPS disponibles (référence pour les volumes SSD à usage général et quantité provisionnée pour les volumes SSD IOPS provisionnés). Vous pouvez ensuite contrôler les performances de votre application et ajuster cette valeur en fonction des exigences de votre application.

L'augmentation de la longueur de file d'attente offre un avantage jusqu'à ce que vous atteigniez le nombre d'IOPS provisionnés, le débit ou la valeur optimale de la longueur de file d'attente du système, actuellement définie sur 32. Par exemple, un volume avec 3 000 IOPS provisionnés doit

cibler une longueur de file d'attente de 3. Vous devez essayer d'augmenter ou de diminuer ces valeurs afin de déterminer ce qui fonctionne le mieux pour votre application.

Longueur de la file d'attente pour les HDD-backed volumes

Pour déterminer la longueur de file d'attente optimale pour votre charge de travail sur les HDD-backed volumes, nous vous recommandons de cibler une longueur de file d'au moins 4 tout en effectuant une exécution séquentielle de 1 Mo. I/Os Vous pouvez ensuite contrôler les performances de votre application et ajuster cette valeur en fonction des exigences de votre application. Par exemple, un st1 volume de 2 TiB avec un débit en rafale de 500 MiB/s et des IOPS de 500 doit cibler une longueur de file d'attente de 4, 8 ou 16 tout en effectuant des opérations séquentielles de 1 024 KiB, 512 KiB ou 256 KiB respectivement. I/Os Vous devez essayer d'augmenter ou de diminuer ces valeurs afin de déterminer ce qui fonctionne le mieux pour votre application.

Désactiver C-states

Avant de lancer l'analyse comparative, vous devez désactiver le processeur C-states. Les cœurs temporairement inactifs d'un processeur compatible peuvent entrer la valeur A C-state pour économiser de l'énergie. Lorsque le cœur est appelé afin de reprendre le traitement, un certain laps de temps est nécessaire avant que le cœur soit à nouveau entièrement opérationnel. Cette latence peut interférer avec les routines de comparaison du processeur. Pour plus d'informations sur les types d'instances EC2 qui les prennent en charge C-states et sur les types d'instances EC2 qui les prennent en charge, consultez la section Contrôle de l'état [du processeur pour votre instance EC2](#).

Instances Linux

Vous pouvez C-states le désactiver sur Amazon Linux, RHEL et CentOS comme suit :

1. Obtenez le numéro de C-states.

```
$ cpupower idle-info | grep "Number of idle states:"
```

2. Désactivez le C-states passage de c1 à cN. Idéalement, l'état des cœurs doit être c0.

```
$ for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

instances Windows

Vous pouvez C-states le désactiver sous Windows de la manière suivante :

1. Dans PowerShell, obtenez le schéma d'alimentation actif actuel.

```
$current_scheme = powercfg /getactivescheme
```

2. Identifiez le GUID du mode de gestion de l'alimentation.

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter "ElementName='High performance']").InstanceID
```

3. Identifiez le GUID du paramètre d'alimentation.

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter "ElementName='Processor idle disable']").InstanceID
```

4. Identifiez le GUID du sous-groupe du paramètre d'alimentation.

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -Filter "ElementName='Processor power management']").InstanceID
```

5. Désactivez C-states en définissant la valeur de l'index sur 1. La valeur 0 indique qu' C-statesils sont désactivés.

```
powercfg /  
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>  
1
```

6. Définissez le schéma actif pour vous assurer que les paramètres sont enregistrés.

```
powercfg /setactive <power_scheme_guid>
```

Effectuer la comparaison

Les procédures suivantes décrivent les commandes de comparaison pour différents types de volume EBS.

Exécutez les commandes suivantes sur une EBS-optimized instance associée à des volumes EBS. Si les volumes EBS ont été créés à partir d'instantanés, veillez à les initialiser avant d'effectuer la comparaison. Pour de plus amples informations, veuillez consulter [Initialiser manuellement les volumes après leur création](#).

 Tip

Vous pouvez utiliser les histogrammes de I/O latence fournis par les statistiques de performances détaillées d'EBS pour comparer la distribution des I/O performances lors de vos tests d'analyse comparative. Pour de plus amples informations, veuillez consulter [Statistiques de performances détaillées d'Amazon EBS](#).

Lorsque vous aurez terminé de tester vos volumes, consultez les rubriques suivantes pour vous aider à nettoyer : [Supprimer un volume Amazon EBS](#) et Mettez [fin à votre instance](#).

Définir des points de référence pour les volumes Provisioned IOPS SSD et SSD à usage général

Instances Linux

Exécutez fio sur la grappe RAID 0 que vous avez créée.

La commande suivante effectue des opérations d'écriture aléatoires 16 Ko.

```
$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --name fio_test_file --direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --group_reporting --norandommap
```

La commande suivante effectue des opérations de lecture aléatoires 16 Ko.

```
$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1 --rw=randread --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --group_reporting --norandommap
```

Pour plus d'informations sur l'interprétation des résultats, consultez le didacticiel [Inspecting disk IO performance with fio](#).

instances Windows

Exécutez DiskSpd sur le volume que vous avez créé.

La commande suivante exécutera un I/O test aléatoire de 30 secondes à l'aide d'un fichier de test de 20 Go situé sur le C : lecteur, avec un ratio d'écriture de 25 % et un ratio de lecture de 75 %, et une taille de bloc de 8 Ko. Il utilisera huit threads de travail, chacun avec quatre en suspens I/Os, et une

valeur d'entropie d'écriture initiale de 1 Go. Les résultats du test seront enregistrés dans un fichier texte appelé `DiskSpeedResults.txt`. Ces paramètres simulent une charge de travail OLTP SQL Server.

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

Pour plus d'informations sur l'interprétation des résultats, consultez le didacticiel [Inspecting disk IO performance with DiskSPd](#).

Volumes **st1** et **sc1** de référence (instances Linux)

Exécutez la commande `fio` sur votre volume **st1** ou **sc1**.

Note

Avant d'exécuter ces tests, définissez buffered I/O sur votre instance comme décrit dans [Augmentez la lecture anticipée pour les charges de travail à haut débit et à lecture intensive sur st1 et sc1 \(Instances Linux uniquement\)](#).

La commande suivante exécute des opérations de lecture séquentielle d'1 Mio sur un périphérique de stockage en mode bloc **st1** attaché (par exemple, `/dev/xvdf`) :

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
--ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

La commande suivante exécute des opérations d'écriture séquentielle d'1 Mio sur un périphérique de stockage en mode bloc **st1** attaché :

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
--ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

Certaines charges de travail exécutent une combinaison de lectures séquentielles et d'écritures séquentielles dans différentes parties du périphérique de stockage en mode bloc. Pour évaluer une telle charge de travail, nous vous recommandons d'utiliser des tâches `fio` distinctes et simultanées pour les lectures et les écritures, et d'utiliser l'option `fio offset_increment` pour cibler différents emplacements du périphérique de stockage en mode bloc pour chaque tâche.

L'exécution de cette charge de travail est un peu plus compliquée qu'une charge de travail d'écriture séquentielle ou de lecture séquentielle. Utilisez un éditeur de texte pour créer un fichier de tâche fio, appelé `fio_rw_mix.cfg` dans cet exemple, contenant les éléments suivants :

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

Ensuite, exécutez la commande suivante :

```
$ sudo fio fio_rw_mix.cfg
```

Pour plus d'informations sur l'interprétation des résultats, consultez ce didacticiel : [Inspecter les I/O performances du disque avec fio](#).

Plusieurs fio tâches en mode direct I/O, même si elles utilisent des opérations de lecture ou d'écriture séquentielles, peuvent entraîner un débit `st1` et des `sc1` volumes inférieurs aux attentes. Nous vous

recommandons d'utiliser une I/O tâche directe et d'utiliser le `iodepth` paramètre pour contrôler le nombre d' I/O opérations simultanées.

Automatisez les sauvegardes avec Amazon Data Lifecycle Manager

Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création, la conservation et la suppression des instantanés EBS et EBS-backed des AMI. Lorsque vous automatisez la gestion des instantanés et des AMI, cela vous aide à :

- protéger les données importantes en appliquant un planning de sauvegarde régulière ;
- créer des AMI standardisées qui peuvent être actualisées à intervalles réguliers ;
- conserver des sauvegardes comme exigé par les auditeurs ou les réglementations internes ;
- réduire les frais de stockage en supprimant les sauvegardes périmées.
- Créez des politiques de sauvegarde de reprise après sinistre qui sauvegardent les données sur des régions ou des comptes isolés.

Combiné à Amazon EventBridge et à la AWS CloudTrail surveillance, Amazon Data Lifecycle Manager fournit une solution de sauvegarde complète pour les instances Amazon EC2 et les volumes EBS sans frais supplémentaires.

Important

- Amazon Data Lifecycle Manager ne peut pas gérer des instantanés ou des AMI créés par d'autres moyens.
- Amazon Data Lifecycle Manager ne peut pas automatiser la création, la conservation et la suppression des AMI basées sur le stockage d'instances.

Amazon Data Lifecycle Manager est considéré comme une fonctionnalité de service d'Amazon Elastic Block Store (Amazon EBS). Tous [AWS les services concernés par un programme de conformité](#) (FedRAMP, HIPAA BAA, SOC, etc.) répertorient Amazon EBS s'appliqueront également à Amazon Data Lifecycle Manager.

Quotas

Votre AWS compte possède les quotas suivants liés à Amazon Data Lifecycle Manager :

Description	Quota
Politiques de cycle de vie personnalisées par région	100
Politiques par défaut pour les instantanés EBS par région	1
Politiques par défaut pour les EBS-backed AMI par région	1
Étiquettes par ressource	45

Fonctionnement de Amazon Data Lifecycle Manager

Voici les éléments de base de Amazon Data Lifecycle Manager.

Éléments

- [Stratégies](#)
- [Calendriers des politiques \(politiques personnalisées uniquement\)](#)
- [Balises de ressources cibles \(politiques personnalisées uniquement\)](#)
- [Instantanés](#)
- [EBS-backed AMI](#)
- [Balises Amazon Data Lifecycle Manager](#)

Stratégies

Avec Amazon Data Lifecycle Manager, vous créez des politiques pour définir vos exigences en matière de création et de conservation des sauvegardes. Ces politiques spécifient généralement les éléments suivants :

- **Type de politique** : définit le type de ressources de sauvegarde que la politique gère (instantanés ou EBS-backed AMI).
- **Ressources cibles** : définit le type de ressources ciblées par la politique (instances ou volumes EBS).

- **Fréquence de création** : définit la fréquence d'exécution de la politique et crée des instantanés ou des AMI.
- **Seuil de conservation** : définit la durée pendant laquelle la politique conserve les instantanés ou les AMI après leur création.
- **Actions supplémentaires** : définit les actions supplémentaires que la politique doit effectuer, comme la copie entre régions, l'archivage ou le balisage des ressources.

Amazon Data Lifecycle Manager propose des politiques par défaut et des politiques personnalisées.

Politiques par défaut

Les politiques par défaut sauvegardent tous les volumes et instances d'une région qui ne disposent pas de sauvegardes récentes. Vous pouvez éventuellement exclure des volumes et des instances en spécifiant des paramètres d'exclusion.

Amazon Data Lifecycle Manager prend en charge les politiques par défaut suivantes :

- **Politique par défaut pour les instantanés EBS** : cible les volumes et automatise la création, la conservation et la suppression des instantanés.
- **Politique par défaut pour les EBS-backed AMI** : cible les instances et automatise la création, la conservation et le désenregistrement des AMI. EBS-backed

Chaque compte et chaque Région AWS ne peuvent contenir qu'une seule politique par défaut par type de ressource.

Politiques personnalisées

Les politiques personnalisées ciblent des ressources spécifiques en fonction des balises qui leur sont attribuées et prennent en charge des fonctionnalités avancées, telles que la restauration rapide des instantanés, l'archivage des instantanés, la copie entre comptes et les pré-scripts et post-scripts. Une politique personnalisée peut inclure jusqu'à 4 planifications, chaque planification pouvant avoir sa propre fréquence de création, son propre seuil de conservation et sa propre configuration de fonctionnalités avancées.

Amazon Data Lifecycle Manager prend en charge les politiques personnalisées suivantes :

- **Politique pour les instantanés EBS** : cible les volumes ou les instances et automatise la création, la conservation et la suppression des instantanés EBS.

- EBS-backed Politique AMI : cible les instances et automatise la création, la conservation et le désenregistrement des AMI. EBS-backed
- Cross-account politique relative aux événements de copie : automatise les actions de copie entre régions pour les instantanés partagés avec vous.

Pour de plus amples informations, veuillez consulter [Politiques par défaut d'Amazon Data Lifecycle Manager par rapport aux politiques personnalisées](#).

Calendriers des politiques (politiques personnalisées uniquement)

Les planifications de politique définissent le moment où les instantanés ou les AMI sont créés par la politique. Les politiques peuvent comporter jusqu'à quatre planifications : une obligatoire et jusqu'à trois facultatives.

L'ajout de plusieurs planifications pour une seule politique vous permet de créer des instantanés ou des AMI à différentes fréquences à l'aide de la même politique. Par exemple, vous pouvez créer une politique unique qui crée des instantanés quotidiens, hebdomadaires, mensuels et annuels. Cela vous évite de devoir gérer plusieurs politiques.

Pour chaque planification, vous pouvez définir la fréquence, les paramètres de restauration d'instantané rapide (politiques de cycle de vie des instantanés uniquement), les règles de copie entre régions et les balises. Les balises affectées à une planification sont automatiquement affectées aux instantanés ou aux images AMI créés lors du lancement de la planification. En outre, Amazon Data Lifecycle Manager attribue automatiquement une balise générée par le système en fonction de la fréquence de la planification à chaque instantané ou AMI.

Chaque planification est lancée individuellement en fonction de sa fréquence. Si plusieurs planifications sont lancées simultanément, Amazon Data Lifecycle Manager ne crée qu'un seul instantané ou une seule AMI et applique les paramètres de rétention de la planification dont la période de rétention est la plus élevée. Les balises de toutes les planifications lancées sont appliquées à l'instantané ou l'AMI.

- (Stratégies de cycle de vie des instantanés uniquement) Si la restauration d'instantané rapide est activée pour plusieurs planifications lancées, l'instantané est activé pour la restauration d'instantané rapide dans toutes les zones de disponibilité spécifiées parmi toutes les planifications lancées. Les paramètres de rétention les plus élevés des planifications lancées sont utilisés pour chaque zone de disponibilité.

- Si plusieurs des planifications lancées sont activées pour la copie entre régions, l'instantané ou l'AMI est copié dans toutes les régions spécifiées dans toutes les planifications lancées. La période de rétention la plus élevée des planifications lancées est appliquée.

Balises de ressources cibles (politiques personnalisées uniquement)

Les politiques personnalisées Amazon Data Lifecycle Manager utilisent des balises de ressource pour identifier les ressources à sauvegarder. Lorsque vous créez un instantané ou une politique EBS-backed AMI, vous pouvez spécifier plusieurs balises de ressources cibles. Toutes les ressources du type spécifié (instance ou volume) qui ont au moins une des balises spécifiées seront retenues par la politique. Par exemple, si vous créez une politique d'instantané qui cible des volumes et que vous spécifiez `purpose=prodcostcenter=prod` et `environment=live` en tant que balises de ressources cibles, la politique ciblera tous les volumes qui possèdent l'une de ces paires clé-valeur de balise.

Si vous souhaitez exécuter plusieurs politiques sur une ressource, vous pouvez attribuer plusieurs balises à la ressource cible, puis créer des politiques distinctes qui ciblent chacune une balise de ressource spécifique.

Vous ne pouvez pas utiliser les caractères \ ou = dans une clé d'identification. Les balises de ressource cible sont sensibles à la casse. Pour plus d'informations, voir [Marquer vos ressources](#).

Instantanés

Les instantanés représentent le principal moyen de sauvegarde des données de vos volumes EBS. Afin d'économiser les frais de stockage, les instantanés successifs sont incrémentiels ; ils contiennent uniquement les données du volume ayant changé depuis l'instantané précédent. Lorsque vous supprimez un instantané dans une série d'instantanés d'un volume, seules les données figurant uniquement dans cet instantané sont supprimées. Le reste de l'historique de capture du volume est conservé. Pour de plus amples informations, veuillez consulter [Instantanés Amazon EBS](#).

EBS-backed AMI

Une Amazon Machine Image (AMI) fournit les informations requises pour lancer une instance. Lorsque vous avez besoin de plusieurs instances configurées de manière identique, il est possible de lancer plusieurs instances à partir d'une même AMI. Amazon Data Lifecycle Manager ne prend en charge que les EBS-backed AMI. Les AMI EBS-backed incluent un instantané pour chaque volume EBS attaché à l'instance source. Pour plus d'informations, consultez [Amazon Machine Images \(AMI\)](#).

Balises Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager applique les balises système suivantes à tous les instantanés et AMI créés par une politique, afin de les distinguer des instantanés et des AMI créés par d'autres moyens :

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime` — Pour les instantanés créés selon une planification basée sur l'âge. Indique quand l'instantané doit être supprimé du niveau standard.
- `dml:managed`
- `aws:dlm:archived` — Pour les instantanés archivés selon une planification.
- `aws:dlm:pre-script` : pour les instantanés créés à l'aide de pré-scripts.
- `aws:dlm:post-script` : pour les instantanés créés à l'aide de post-scripts.

Vous pouvez également spécifier des balises personnalisées à appliquer aux instantanés et aux AMI au moment de leur création. Vous ne pouvez pas utiliser les caractères \ ou = dans une clé d'identification.

Les balises cible utilisées par Amazon Data Lifecycle Manager pour associer des volumes à une politique d'instantanés peuvent éventuellement être appliquées aux instantanés créés par la politique. De même, les balises cibles utilisées pour associer des instances à une politique AMI peuvent éventuellement être appliquées aux AMI créées par la politique.

Politiques par défaut d'Amazon Data Lifecycle Manager par rapport aux politiques personnalisées

Cette section compare les politiques par défaut et les politiques personnalisées et met en évidence leurs similitudes et leurs différences.

Rubriques

- [Comparaison des politiques d'instantanés EBS](#)
- [EBS-backed Comparaison des politiques AMI](#)

Comparaison des politiques d'instantanés EBS

Le tableau suivant met en évidence les différences entre la politique d'instantanés EBS par défaut et les politiques d'instantanés EBS personnalisées.

Fonctionnalité	Politique par défaut pour les instantanés EBS	Politique d'instantanés EBS personnalisée
Ressource de sauvegarde gérée	Instantané EBS	Instantané EBS
Types de ressources cibles	Volumes	Volumes ou instances
Ciblage des ressources	Cible tous les volumes de la région qui n'ont pas d'instantanés récents. Vous pouvez définir des paramètres d'exclusion pour exclure des volumes spécifiques.	Cible uniquement les volumes ou les instances dotés de balises spécifiques.
Paramètres d'exclusion	Oui, il est possible d'exclure des volumes de démarrage, des types de volumes spécifiques et des volumes dotés de balises spécifiques.	Oui, il est possible d'exclure des volumes de démarrage et des volumes dotés de balises spécifiques lors du ciblage des instances.
Support AWS Outposts	Non	Oui
Prise en charge de plusieurs planifications	Non	Oui, jusqu'à 4 planifications par politique
Types de conservation pris en charge	Age-based rétention uniquement	Age-based et rétention basée sur le nombre

Fonctionnalité	Politique par défaut pour les instantanés EBS	Politique d'instantanés EBS personnalisée
Fréquence de création d'instantanés	Tous les 1 à 7 jours.	Fréquence quotidienne, hebdomadaire, mensuelle, annuelle ou personnalisée à l'aide d'une expression cron.
Conservation des instantanés	2 à 14 jours.	Jusqu'à 1 000 instantanés (basée sur le nombre) ou 100 ans (basée sur l'âge).
Prise en charge des instantanés cohérents par rapport à l'application	Non	Oui, en utilisant des pré-scripts et des post-scripts
Prise en charge de l'archivage des instantanés	Non	Oui
Prise en charge de la restauration d'instantané rapide	Non	Oui
Prise en charge de la copie entre régions	Oui, avec les paramètres par défaut ¹	Oui, avec des paramètres personnalisés
Prise en charge du partage entre comptes	Non	Oui
Prise en charge de la suppression prolongée ²	Oui	Non

¹ Pour les politiques par défaut :

- Vous ne pouvez pas copier les balises dans des copies entre régions.
- Les copies utilisent la même période de conservation que l'instantané source.
- Les copies ont le même état de chiffrement que l'instantané source. Si le chiffrement est activé par défaut dans la région de destination, les copies sont toujours chiffrées, même si les instantanés source ne sont pas chiffrés. Les copies sont toujours chiffrées avec la clé KMS par défaut pour la région de destination.

² Pour les politiques par défaut et personnalisées :

- Si une instance ou un volume cible est supprimé, Amazon Data Lifecycle Manager continue de supprimer les instantanés jusqu'au dernier, mais sans l'inclure, en se basant sur la période de conservation. Pour les politiques par défaut, vous pouvez étendre la suppression pour inclure le dernier instantané.
- Si une politique est supprimée ou passe à l'état d'erreur ou de désactivation, Amazon Data Lifecycle Manager arrête de supprimer les instantanés. Pour les politiques par défaut, vous pouvez étendre la suppression pour continuer de supprimer les instantanés, y compris le dernier.

EBS-backed Comparaison des politiques AMI

Le tableau suivant met en évidence les différences entre la politique par défaut pour les EBS-backed AMI et les politiques EBS-backed AMI personnalisées.

Fonctionnalité	Politique par défaut pour les EBS-backed AMI	Politique EBS-backed AMI personnalisée
Ressource de sauvegarde gérée	EBS-backed AMI	EBS-backed AMI
Types de ressources cibles	instances	instances
Ciblage des ressources	Cible toutes les instances de la région qui n'ont pas d'AMI récentes.	Cible uniquement les instances dotées de balises spécifiques.

Fonctionnalité	Politique par défaut pour les EBS-backed AMI	Politique EBS-backed AMI personnalisée
	Vous pouvez définir des paramètres d'exclusion pour exclure des instances spécifiques.	
Redémarrage des instances avant la création de l'AMI	Non	Oui
Paramètres d'exclusion	Oui, il est possible d'exclure des instances dotées de balises spécifiques.	Non
Prise en charge de plusieurs planifications	Non	Oui, jusqu'à 4 planifications par politique.
Fréquence de création des AMI	Tous les 1 à 7 jours.	Fréquence quotidienne, hebdomadaire, mensuelle, annuelle ou personnalisée à l'aide d'une expression cron.
Types de conservation pris en charge	Age-based rétention uniquement.	Age-based et une rétention basée sur le décompte.
Conservation des AMI	2 à 14 jours.	Jusqu'à 1 000 AMI (basée sur le nombre) ou 100 ans (basée sur l'âge).
Prise en charge de l'obsolescence des AMI	Non	Oui
Prise en charge de la copie entre régions	Oui, avec les paramètres par défaut ¹	Oui, avec des paramètres personnalisés

Fonctionnalité	Politique par défaut pour les EBS-backed AMI	Politique EBS-backed AMI personnalisée
Prise en charge de la suppression prolongée ²	Oui	Non

¹ Pour les politiques par défaut :

- Vous ne pouvez pas copier les balises dans des copies entre régions.
- Les copies utilisent la même période de conservation que l'AMI source.
- Les copies ont le même état de chiffrement que l'AMI source. Si le chiffrement est activé par défaut dans la région de destination, les copies sont toujours chiffrées, même si les AMI source ne sont pas chiffrées. Les copies sont toujours chiffrées avec la clé KMS par défaut pour la région de destination.

² Pour les politiques par défaut et personnalisées :

- Si une instance ciblée est résiliée, Amazon Data Lifecycle Manager continue l'annulation de l'inscription des AMI jusqu'à la dernière, mais sans l'inclure, en se basant sur la période de conservation. Pour les politiques par défaut, vous pouvez étendre l'annulation de l'inscription pour inclure la dernière AMI.
- Si une politique est supprimée ou passe à l'état d'erreur ou de désactivation, Amazon Data Lifecycle Manager arrête d'annuler l'inscription des AMI. Pour les politiques par défaut, vous pouvez étendre la suppression pour continuer d'annuler l'inscription des AMI, y compris la dernière.

Création de politiques par défaut pour Amazon Data Lifecycle Manager

Pour créer des EBS-backed AMI périodiques à partir d'instances, utilisez la politique par défaut pour les EBS-backed AMI. Pour créer des instantanés de tous les volumes, quel que soit leur état d'attachement, ou si vous souhaitez exclure des volumes spécifiques, utilisez la politique par défaut pour les instantanés EBS.

Cette section explique comment créer des politiques par défaut.

Rubriques

- [Considérations relatives aux politiques par défaut](#)
- [Création d'une politique par défaut pour les instantanés Amazon EBS](#)
- [Création d'une politique par défaut pour les EBS-backed AMI](#)
- [Activez les politiques par défaut de Data Lifecycle Manager pour tous les comptes et toutes les régions](#)

Considérations relatives aux politiques par défaut

Gardez ce qui suit à l'esprit lorsque vous utilisez des politiques par défaut :

- Les politiques par défaut ne sauvegardent pas les ressources cibles (instances ou volumes) ayant fait l'objet de sauvegardes récentes (instantanés ou AMI). La fréquence de création détermine les ressources sauvegardées. Un volume ou une instance n'est sauvegardé que si son dernier instantané ou sa dernière AMI date d'avant la fréquence de création de la politique. Par exemple, si vous spécifiez une fréquence de création de 3 jours, la politique par défaut pour les instantanés EBS créera un instantané d'un volume uniquement si le dernier instantané date de plus de 3 jours.
- Par défaut, les politiques par défaut ciblent toutes les instances ou tous les volumes de la région, sauf si des paramètres d'exclusion sont spécifiés.
- Les politiques par défaut créeront un ensemble minimal d'instantanés uniques. Par exemple, si vous activez la politique EBS-backed AMI et la politique de capture instantanée EBS, la politique de capture instantanée ne dupliquera pas les instantanés des volumes déjà sauvegardés par la politique EBS-backed AMI.
- Les politiques par défaut ne commenceront à cibler que les ressources datant d'au moins 24 heures.
- Si vous supprimez un volume ou que vous résiliez une instance ciblée par une politique par défaut, Amazon Data Lifecycle Manager continue de supprimer les sauvegardes précédemment créées (instantanés ou AMI) en fonction de la période de conservation jusqu'à la dernière sauvegarde, mais sans l'inclure. Vous devez supprimer manuellement cette sauvegarde si elle n'est pas nécessaire.

Si vous souhaitez qu'Amazon Data Lifecycle Manager supprime la dernière sauvegarde, vous pouvez activer la suppression étendue.

- Si une politique par défaut est supprimée ou passe à l'état d'erreur ou de désactivation, Amazon Data Lifecycle Manager arrête de supprimer les sauvegardes précédemment créées (instantanés

ou AMI). Si vous souhaitez qu'Amazon Data Lifecycle Manager continue de supprimer des sauvegardes, y compris la dernière, vous devez activer la suppression étendue avant de supprimer la politique ou avant que la politique ne passe à l'état de désactivation ou de suppression.

- Lorsque vous créez et activez une politique par défaut, Amazon Data Lifecycle Manager affecte de manière aléatoire des ressources ciblées à une fenêtre horaire de quatre heures. Les ressources ciblées sont sauvegardées pendant la fenêtre qui leur est attribuée à la fréquence de création spécifiée. Par exemple, si une politique a une fréquence de création de 3 jours et que la fenêtre 12 h 00 – 16 h 00 est attribuée à une ressource cible, cette ressource sera sauvegardée entre 12 h 00 et 16 h 00 tous les 3 jours.

Création d'une politique par défaut pour les instantanés Amazon EBS

La procédure suivante vous explique comment créer une politique par défaut pour les instantanés EBS.

Console

Pour créer une politique par défaut pour les instantanés EBS

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie.
3. Pour Type de stratégie, choisissez Stratégie par défaut, puis Politique d'instantané EBS.
4. Pour Description, saisissez une brève description pour la stratégie.
5. Pour Rôle IAM, sélectionnez le rôle IAM disposant d'autorisations pour gérer les instantanés.

Nous vous recommandons de choisir Par défaut pour utiliser le rôle IAM par défaut fourni par Amazon Data Lifecycle Manager. Toutefois, vous pouvez également utiliser un rôle IAM personnalisé que vous avez créé précédemment.

6. Pour Fréquence de création, spécifiez la fréquence à laquelle vous souhaitez que la politique s'exécute et crée des instantanés de vos volumes.

La fréquence que vous spécifiez détermine également les volumes sauvegardés. La politique ne sauvegardera que les volumes qui n'ont pas été sauvegardés par un autre moyen selon la fréquence spécifiée. Par exemple, si vous spécifiez une fréquence de création de 3 jours, la politique créera uniquement des instantanés des volumes qui n'ont pas été sauvegardés au cours des 3 derniers jours.

7. Pour Période de conservation, spécifiez la durée pendant laquelle vous souhaitez que la politique conserve les instantanés qu'elle crée. Lorsqu'un instantané atteint le seuil de conservation, il est automatiquement supprimé. La période de conservation doit être supérieure ou égale à la fréquence de création.
8. (Facultatif) Configurez les Paramètres d'exclusion pour exclure des volumes spécifiques des sauvegardes planifiées. Les volumes exclus ne seront pas sauvegardés lors de l'exécution de la politique.
 - a. Pour exclure les volumes de démarrage, sélectionnez Exclure les volumes de démarrage. Si vous excluez les volumes de démarrage, seuls les volumes de données (autres que les volumes de démarrage) seront sauvegardés conformément à la politique. En d'autres termes, la politique ne créera pas d'instantanés des volumes attachés à des instances en tant que volume de démarrage.
 - b. Pour exclure des types de volumes spécifiques, choisissez Exclure des types de volumes spécifiques, puis sélectionnez les types de volumes à exclure. Seuls les volumes des types restants seront sauvegardés par la politique.
 - c. Pour exclure les volumes dotés de balises spécifiques, choisissez Ajouter une balise, puis spécifiez les clés et les valeurs des balises. La politique ne créera pas d'instantanés des volumes qui ont l'une des balises spécifiées.
9. (Facultatif) Dans les Paramètres avancés, spécifiez les actions supplémentaires que la politique doit effectuer.
 - a. Pour copier les balises attribuées des volumes source vers leurs instantanés, sélectionnez Copier les balises depuis les volumes.
 - b. Lorsque l'option Étendre la suppression est désactivée :
 - Si un volume source est supprimé, Amazon Data Lifecycle Manager continue de supprimer les instantanés précédemment créés jusqu'au dernier, mais sans l'inclure, en se basant sur la période de conservation. Si vous souhaitez qu'Amazon Data Lifecycle Manager supprime tous les instantanés, y compris le dernier, sélectionnez Étendre la suppression.
 - Si une politique est supprimée ou passe à l'état `error` ou `disabled`, Amazon Data Lifecycle Manager arrête de supprimer les instantanés. Si vous souhaitez qu'Amazon Data Lifecycle Manager continue de supprimer les instantanés, y compris le dernier, sélectionnez Étendre la suppression.

 Note

Si vous activez la suppression étendue, vous remplacez simultanément les deux comportements décrits ci-dessus.

- c. Pour copier les instantanés créés par la politique vers d'autres régions, sélectionnez Créer une copie entre régions, puis sélectionnez jusqu'à 3 régions de destination.
 - Si l'instantané source est chiffré ou si le chiffrement par défaut est activé pour la région de destination, les instantanés copiés sont chiffrés à l'aide de la clé KMS par défaut pour le chiffrement EBS dans la région de destination.
 - Si l'instantané source n'est pas chiffré et que le chiffrement par défaut est désactivé pour la région de destination, les instantanés copiés ne sont pas chiffrés.
10. (Facultatif) Pour ajouter une balise à la politique, choisissez Ajouter une balise et saisissez la paire de clé et de valeur de la balise.
11. Choisissez Créer une politique par défaut.

 Note

Si vous obtenez l'erreur `Role with name AWSDatalifecycleManagerDefaultRole already exists`, consultez [Résoudre les problèmes liés à Amazon Data Lifecycle Manager](#) pour plus d'informations.

AWS CLI

Pour créer une politique par défaut pour les instantanés EBS

Utilisez la commande [create-lifecycle-policy](#). Vous pouvez spécifier les paramètres de la requête selon l'une des deux méthodes suivantes, en fonction de votre cas d'utilisation ou de vos préférences :

- Méthode 1 :

```
$ aws dlm create-lifecycle-policy \  
--state ENABLED | DISABLED \  

```



```
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeBootVolumes=true | false,
ExcludeTags=[{Key=tag_key,Value=tag_value}], ExcludeVolumeTypes="standard | gp2 |
gp3 | io1 | io2 | st1 | sc1"
```

Par exemple, pour créer une politique par défaut pour les instantanés EBS qui cible tous les volumes de la région, qui utilise le rôle IAM par défaut, qui s'exécute quotidiennement (par défaut) et qui conserve les instantanés pendant 7 jours (par défaut), vous devez spécifier les paramètres suivants :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default snapshot policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRole \
--default-policy VOLUME
```

- Méthode 2 :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--policy-details file://policyDetails.json
```

Où `policyDetails.json` inclut les éléments suivants :

```
{
  "PolicyLanguage": "SIMPLIFIED",
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceType": "VOLUME",
  "CopyTags": true | false,
  "CreateInterval": creation_frequency_in_days (1-7),
  "RetainInterval": retention_period_in_days (2-14),
```

```

    "ExtendDeletion": true | false,
    "CrossRegionCopyTargets": [{"TargetRegion": "destination_region_code"}],
    "Exclusions": {
        "ExcludeBootVolume": true | false,
        "ExcludeVolumeTypes": ["standard | gp2 | gp3 | io1 | io2 | st1 | sc1"],
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}

```

Création d'une politique par défaut pour les EBS-backed AMI

La procédure suivante vous montre comment créer une politique par défaut pour les EBS-backed AMI.

Console

Pour créer une politique par défaut pour les EBS-backed AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie.
3. Pour Type de stratégie, choisissez Stratégie par défaut, puis choisissez EBS-backed Stratégie AMI.
4. Pour Description, saisissez une brève description pour la stratégie.
5. Pour Rôle IAM, sélectionnez le rôle IAM disposant d'autorisations pour gérer les AMI.

Nous vous recommandons de choisir Par défaut pour utiliser le rôle IAM par défaut fourni par Amazon Data Lifecycle Manager. Toutefois, vous pouvez également utiliser un rôle IAM personnalisé que vous avez créé précédemment.

6. Pour Fréquence de création, spécifiez la fréquence à laquelle vous souhaitez que la politique s'exécute et crée des AMI à partir de vos instances.

La fréquence que vous spécifiez détermine également les instances sauvegardées. La politique ne sauvegardera que les instances qui n'ont pas été sauvegardées par un autre moyen selon la fréquence spécifiée. Par exemple, si vous spécifiez une fréquence de

création de 3 jours, la politique créera uniquement des AMI à partir des instances qui n'ont pas été sauvegardées au cours des 3 derniers jours.

7. Pour Période de conservation, spécifiez la durée pendant laquelle vous souhaitez que la politique conserve les AMI qu'elle crée. Lorsqu'une AMI atteint le seuil de conservation, son inscription est automatiquement annulée et ses instantanés associés sont supprimés. La période de conservation doit être supérieure ou égale à la fréquence de création.
8. (Facultatif) Configurez les Paramètres d'exclusion pour exclure des instances spécifiques des sauvegardes planifiées. Les instances exclues ne seront pas sauvegardées lors de l'exécution de la politique.
 - Pour exclure les instances dotées de balises spécifiques, choisissez Ajouter une balise, puis spécifiez les clés et les valeurs des balises. La politique ne créera pas d'AMI à partir des instances dotées de l'une des balises spécifiées.
9. (Facultatif) Dans les Paramètres avancés, spécifiez les actions supplémentaires que la politique doit effectuer.
 - a. Pour copier les balises attribuées depuis les instances sources vers leurs AMI, sélectionnez Copier les balises depuis les instances.
 - b. Lorsque l'option Étendre la suppression est désactivée :
 - Si une instance source est résiliée, Amazon Data Lifecycle Manager continue d'annuler l'inscription des AMI précédemment créées jusqu'à la dernière, mais sans l'inclure, en se basant sur la période de conservation. Si vous souhaitez qu'Amazon Data Lifecycle Manager annule l'inscription de toutes les AMI, y compris la dernière, sélectionnez Étendre la suppression.
 - Si une politique est supprimée ou passe à l'état `error` ou `disabled`, Amazon Data Lifecycle Manager arrête d'annuler l'inscription des AMI. Si vous souhaitez qu'Amazon Data Lifecycle Manager continue d'annuler l'inscription des AMI, y compris la dernière, sélectionnez Étendre la suppression.

 Note

Si vous activez la suppression étendue, vous remplacez simultanément les deux comportements décrits ci-dessus.

- c. Pour copier les AMI créées par la politique vers d'autres régions, sélectionnez Créer une copie entre régions, puis sélectionnez jusqu'à 3 régions de destination.
 - Si l'AMI source est chiffrée ou si le chiffrement par défaut est activé pour la région de destination, les AMI copiées sont chiffrées à l'aide de la clé KMS par défaut pour le chiffrement EBS dans la région de destination.
 - Si l'AMI source n'est pas chiffrée et que le chiffrement par défaut est désactivé pour la région de destination, les AMI copiées ne sont pas chiffrées.
10. (Facultatif) Pour ajouter une balise à la politique, choisissez Ajouter une balise et saisissez la paire de clé et de valeur de la balise.
11. Choisissez Créer une politique par défaut.

 Note

Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, consultez [Résoudre les problèmes liés à Amazon Data Lifecycle Manager](#) pour plus d'informations.

AWS CLI

Pour créer une politique par défaut pour les EBS-backed AMI

Utilisez la commande [create-lifecycle-policy](#). Vous pouvez spécifier les paramètres de la requête selon l'une des deux méthodes suivantes, en fonction de votre cas d'utilisation ou de vos préférences :

- Méthode 1 :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
```

```
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeTags=[{Key=tag_key,Value=tag_value}]
```

Par exemple, pour créer une politique par défaut pour les EBS-backed AMI qui cible toutes les instances de la région, utilise le rôle IAM par défaut, s'exécute quotidiennement (par défaut) et conserve les AMI pendant 7 jours (par défaut), vous devez spécifier les paramètres suivants :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default AMI policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--default-policy INSTANCE
```

- Méthode 2 :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--policy-details file://policyDetails.json
```

Où `policyDetails.json` inclut les éléments suivants :

```
{
  "PolicyLanguage": "SIMPLIFIED",
  "PolicyType": "IMAGE_MANAGEMENT",
  "ResourceType": "INSTANCE",
  "CopyTags": true | false,
  "CreateInterval": creation_frequency_in_days (1-7),
  "RetainInterval": retention_period_in_days (2-14),
  "ExtendDeletion": true | false,
  "CrossRegionCopyTargets": [{"TargetRegion": "destination_region_code"}],
  "Exclusions": {
    "ExcludeTags": [{
      "Key": "exclusion_tag_key",
      "Value": "exclusion_tag_value"
    }]
  }
}
```

Activez les politiques par défaut de Data Lifecycle Manager pour tous les comptes et toutes les régions

À l'aide de CloudFormation StackSets, vous pouvez activer les politiques par défaut d'Amazon Data Lifecycle Manager pour plusieurs comptes et AWS régions en une seule opération.

Vous pouvez utiliser des ensembles de piles pour activer les politiques par défaut de l'une des manières suivantes :

- Dans l'ensemble de AWS l'organisation : garantit que les politiques par défaut sont activées et configurées de manière cohérente dans AWS l'ensemble de l'organisation ou dans des unités organisationnelles spécifiques d'une organisation. Cela se fait à l'aide des autorisations gérées par les services. CloudFormation StackSets crée les rôles IAM requis en votre nom.
- Sur des AWS comptes spécifiques : garantit que les politiques par défaut sont activées et configurées de manière cohérente sur des comptes cibles spécifiques. Cela nécessite des autorisations autogérées. Vous créez les rôles IAM nécessaires pour établir la relation de confiance entre le compte administrateur du stack set et les comptes cibles.

Pour plus d'informations, consultez la section Modèles [d'autorisation pour les ensembles de piles](#) dans le Guide de AWS CloudFormation l'utilisateur.

Utilisez les procédures suivantes pour activer les politiques par défaut d'Amazon Data Lifecycle Manager pour AWS l'ensemble d'une organisation, pour des unités d'organisation spécifiques ou pour des comptes cibles spécifiques.

Conditions préalables

Effectuez l'une des opérations suivantes, en fonction de la manière dont vous activez les politiques par défaut :

- (Dans toutes AWS les organisations) Vous devez [activer toutes les fonctionnalités de votre organisation](#) et [activer l'accès sécurisé avec AWS Organizations](#). Vous devez également utiliser le compte de gestion de l'organisation ou un compte d'administrateur [délégué](#).
- (Sur des comptes cibles spécifiques) Vous devez [accorder des autorisations autogérées](#) en créant les rôles nécessaires pour établir une relation de confiance entre le compte administrateur du stack set et les comptes cibles.

Console

Pour activer les politiques par défaut sur AWS organisation ou sur des comptes cibles spécifiques

1. Ouvrez la CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
 2. Dans le volet de navigation, choisissez `StackSets`, puis choisissez `Créer StackSet`.
 3. Pour les autorisations, effectuez l'une des opérations suivantes, en fonction de la manière dont vous activez les politiques par défaut :
 - (Au sein d'une AWS organisation) Choisissez `Service-managed les autorisations`.
 - (Sur des comptes cibles spécifiques) Choisissez `Self-service les autorisations`. Ensuite, pour l'ARN du rôle d'administrateur IAM, sélectionnez le rôle de service IAM que vous avez créé pour le compte administrateur, et pour le nom du rôle d'exécution IAM, entrez le nom du rôle de service IAM que vous avez créé dans les comptes cibles.
 4. Pour Préparer un modèle, choisissez `Utiliser un exemple de modèle`.
 5. Pour les exemples de modèles, effectuez l'une des opérations suivantes :
 - (Politique par défaut pour les instantanés EBS) Sélectionnez `Créer les politiques par défaut d'Amazon Data Lifecycle Manager pour les instantanés EBS`.
 - (Politique par défaut pour les EBS-backed AMI) Sélectionnez `Créer les politiques par défaut d'Amazon Data Lifecycle Manager pour les EBS-backed AMI`.
 6. Choisissez `Suivant`.
 7. Pour `StackSet le nom` et `StackSet la description`, entrez un nom descriptif et une brève description.
 8. Dans la section `Paramètres`, configurez les paramètres de stratégie par défaut selon vos besoins.
- 
- ### Note
- Pour les charges de travail critiques, nous recommandons `CreateInterval = 1 jour` et `RetainInterval = 7 jours`.
9. Choisissez `Suivant`.
 10. (Facultatif) Pour les balises, spécifiez des balises pour vous aider à identifier les ressources `StackSet` et à les empiler.

11. Pour Exécution gérée, choisissez Active.
12. Choisissez Suivant.
13. Pour Add stacks to stack set (Ajouter des piles à un ensemble de piles), sélectionnez Deploy new stacks (Déployer de nouvelles piles).
14. Effectuez l'une des opérations suivantes, en fonction de la manière dont vous activez les politiques par défaut :
 - (Dans toute AWS l'organisation) Pour les cibles de déploiement, choisissez l'une des options suivantes :
 - Pour déployer dans l'ensemble d'une AWS organisation, choisissez Déployer dans l'organisation.
 - Pour déployer vers des unités organisationnelles (UO) spécifiques, choisissez Déployer vers des unités organisationnelles, puis pour ID d'unité organisationnelle, entrez l'ID de l'unité d'organisation. Pour ajouter des unités d'organisation supplémentaires, choisissez Ajouter une autre unité d'organisation.
 - (Sur des comptes cibles spécifiques) Pour les comptes, effectuez l'une des opérations suivantes :
 - Pour déployer sur des comptes cibles spécifiques, choisissez Déployer des piles dans les comptes, puis dans Numéros de compte, entrez les ID des comptes cibles.
 - Pour déployer sur tous les comptes d'une unité d'organisation spécifique, choisissez Déployer la pile sur tous les comptes d'une unité organisationnelle, puis dans Numéros d'organisation, entrez l'ID de l'unité d'organisation cible.
15. Pour le déploiement automatique, choisissez Activé.
16. Pour Comportement en matière de suppression de compte, choisissez Retain stacks.
17. Pour Spécifier les régions, sélectionnez des régions spécifiques dans lesquelles activer les politiques par défaut, ou choisissez Ajouter toutes les régions pour activer les politiques par défaut dans toutes les régions.
18. Choisissez Suivant.
19. Vérifiez les paramètres de l'ensemble de piles, sélectionnez Je reconnais que cela CloudFormation peut créer des ressources IAM, puis choisissez Soumettre.

AWS CLI

Pour activer les politiques par défaut sur AWS organization

1. Créez le stack set. Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-stack-set.html> `create-stack-set`.

Pour `--permission-model`, spécifiez `SERVICE_MANAGED`.

Pour `--template-url`, spécifiez l'un des modèles d'URL suivants :

- (Politiques par défaut pour les EBS-backed AMI) <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml>
- (Politiques par défaut pour les instantanés EBS) <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml>

Pour `--parameters`, spécifiez les paramètres des politiques par défaut. Pour les paramètres pris en charge, les descriptions des paramètres et les valeurs valides, téléchargez le modèle à l'aide de l'URL, puis visualisez-le à l'aide d'un éditeur de texte.

Pour `--auto-deployment`, spécifiez `Enabled=true`, `RetainStacksOnAccountRemoval=true`.

```
$ aws cloudformation create-stack-set \  
--stack-set-name stackset_name \  
--permission-model SERVICE_MANAGED \  
--template-url template_url \  
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1" \  
              "ParameterKey=param_name_2,ParameterValue=param_value_2" \  
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Déployez le stack set. Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-stack-instances.html> `create-stack-instances`.

Pour `--stack-set-name`, spécifiez le nom de l'ensemble de piles que vous avez créé à l'étape précédente.

Pour `--deployment-targets OrganizationalUnitIds`, spécifiez l'ID de l'unité d'organisation racine à déployer sur l'ensemble de l'organisation, ou les ID d'unité d'organisation à déployer sur des unités d'organisation spécifiques de l'organisation.

Pour `--regions`, spécifiez les AWS régions dans lesquelles activer les politiques par défaut.

```
$ aws cloudformation create-stack-instances \  
--stack-set-name stackset_name \  
--deployment-targets OrganizationalUnitIds='["root_ou_id"]' | '["ou_id_1",  
"ou_id_2"]' \  
--regions '["region_1", "region_2"]'
```

Pour activer les politiques par défaut sur des comptes cibles spécifiques

1. Créez le stack set. Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-stack-set.html> `create-stack-set`.

Pour `--template-url`, spécifiez l'un des modèles d'URL suivants :

- (Politiques par défaut pour les EBS-backed AMI) <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml>
- (Politiques par défaut pour les instantanés EBS) <https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml>

Pour `--administration-role-arn`, spécifiez l'ARN du rôle de service IAM que vous avez créé précédemment pour l'administrateur du stack set.

Pour `--execution-role-name`, spécifiez le nom du rôle de service IAM que vous avez créé dans les comptes cibles.

Pour `--parameters`, spécifiez les paramètres des politiques par défaut. Pour les paramètres pris en charge, les descriptions des paramètres et les valeurs valides, téléchargez le modèle à l'aide de l'URL, puis visualisez-le à l'aide d'un éditeur de texte.

Pour `--auto-deployment`, spécifiez `Enabled=true`, `RetainStacksOnAccountRemoval=true`.

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
"ParameterKey=param_name_2,ParameterValue=param_value_2" \
--administration-role-arn administrator_role_arn \
--execution-role-name target_account_role \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Déployez le stack set. Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/cloudformation/create-stack-instances.html> `create-stack-instances`.

Pour `--stack-set-name`, spécifiez le nom de l'ensemble de piles que vous avez créé à l'étape précédente.

Pour `--accounts`, spécifiez les ID des AWS comptes cibles.

Pour `--regions`, spécifiez les AWS régions dans lesquelles activer les politiques par défaut.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--accounts '["account_ID_1", "account_ID_2"]' \
--regions '["region_1", "region_2"]'
```

Création d'une politique personnalisée Amazon Data Lifecycle Manager pour les instantanés EBS

La procédure suivante montre comment utiliser Amazon Data Lifecycle Manager pour automatiser les cycles de vie des instantanés Amazon EBS.

Rubriques

- [Pour créer une stratégie de cycle de vie d'instantané](#)
- [Considérations relatives aux stratégies de cycle de vie des instantanés](#)
- [Ressources supplémentaires](#)
- [Automatisez les instantanés cohérents avec les applications avec Data Lifecycle Manager](#)
- [Autres cas d'utilisation des pré-scripts et des post-scripts de Data Lifecycle Manager](#)
- [Comment fonctionnent les pré-scripts et les post-scripts d'Amazon Data Lifecycle Manager](#)

- [Identifiez les instantanés créés avec les pré-scripts et les post-scripts de Data Lifecycle Manager](#)
- [Surveillez les pré-scripts et les post-scripts d'Amazon Data Lifecycle Manager](#)

Pour créer une stratégie de cycle de vie d'instantané

Suivez l'une des procédures suivantes pour créer une politique de cycle de vie des instantanés.

Console

Pour créer une politique d'instantané

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans la page Sélectionner un type de stratégie, choisissez Stratégie d'instantané EBS, puis Suivant.
4. Dans la section Ressources cibles, effectuez les opérations suivantes :
 - a. Pour Types de ressource cibles, choisissez le type de ressource à sauvegarder. Sélectionnez Volume pour créer des instantanés de volumes individuels, ou Instance pour créer des instantanés multi-volume à partir des volumes d'une instance.
 - b. (Outpost et clients de la zone locale uniquement) Spécifiez l'emplacement des ressources cibles.

Pour Emplacement de la ressource cible, spécifiez l'emplacement des ressources cibles.

- Pour cibler les ressources d'une région, choisissez AWS Région. Amazon Data Lifecycle Manager sauvegardera toutes les ressources du type spécifié qui ont des balises cibles correspondantes dans la région actuelle uniquement. Les instantanés sont créés dans la même région.
- Pour cibler les ressources dans les zones locales, choisissez AWS Local Zones. Amazon Data Lifecycle Manager sauvegardera toutes les ressources du type spécifié qui ont des balises cibles correspondantes dans toutes les zones locales de la région actuelle uniquement. Les instantanés peuvent être créés dans la même zone locale que la ressource source ou dans sa région parente.
- Pour cibler les ressources Outpost et, choisissez AWS Outpost. Amazon Data Lifecycle Manager sauvegardera toutes les ressources du type spécifié dont les

balises cibles correspondent à l'ensemble Outposts de votre compte. Les instantanés peuvent être créés sur la même ressource Outpost que la ressource source ou dans sa région parente.

- c. Pour Etiquettes de ressources cibles, choisissez les étiquettes de ressources qui identifient les volumes ou les instances à sauvegarder. Seules les ressources qui ont la clé de balise et les paires de valeurs spécifiées sont sauvegardées par la politique.
5. Pour Description, saisissez une brève description pour la stratégie.
6. Pour Rôle IAM, choisissez le rôle IAM autorisé à gérer des instantanés, ainsi qu'à décrire des volumes et des instances. Pour utiliser le rôle par défaut fourni par Amazon Data Lifecycle Manager, choisissez Rôle par défaut. Autrement, pour utiliser un rôle IAM personnalisé que vous avez créé précédemment, sélectionnez Choisir un autre rôle, puis sélectionnez le rôle à utiliser.
7. Pour Etiquettes de stratégie, ajoutez les étiquettes à appliquer à la stratégie de cycle de vie. Vous pouvez utiliser ces étiquettes pour identifier et catégoriser vos politiques.
8. Pour Policy status (Statut de la politique), choisissez Enable (Activer) pour lancer l'exécution de la politique à la prochaine heure planifiée, ou Disable policy (Désactiver la politique) pour empêcher l'exécution de la politique. Si vous n'activez pas la politique maintenant, elle ne commencera à créer des instantanés que quand vous l'aurez activée manuellement après sa création.
9. (Politiques qui ciblent uniquement les instances) Excluez les volumes des ensembles d'instantanés multi-volumes.

Par défaut, Amazon Data Lifecycle Manager créera des instantanés de tous les volumes attachés aux instances ciblées. Cependant, vous pouvez choisir de créer des instantanés d'un sous-ensemble des volumes attachés. Dans la section Parameters (Paramètres), procédez comme suit :

- Si vous ne voulez pas créer d'instantanés des volumes racines attachés aux instances ciblées, sélectionnez Exclude root volume (Exclure le volume racine). Si vous sélectionnez cette option, seuls les volumes de données (non racine) attachés aux instances ciblées seront inclus dans les ensembles instantanés multi-volumes.
- Si vous voulez créer des instantanés d'un sous-ensemble de volumes de données (non racine) attachés aux instances ciblées, sélectionnez Exclude specific data volumes (Exclure des volumes de données spécifiques), puis spécifiez les identifications à utiliser pour identifier les volumes de données qui ne doivent pas faire l'objet d'un instantané. Amazon Data Lifecycle Manager ne créera pas d'instantanés des volumes de données qui

ont l'une des identifications spécifiées. Amazon Data Lifecycle Manager créera uniquement des instantanés des volumes de données qui n'ont aucune des identifications spécifiées.

10. Choisissez Suivant.

11. Dans l'écran Configurer une planification, configurez les planifications de stratégie. Une politique peut avoir jusqu'à 4 planifications. La planification 1 est obligatoire. Les planifications 2, 3 et 4 sont facultatives. Pour chaque planification de politique que vous ajoutez, procédez comme suit :

- a. Dans la section Détails de la planification, procédez comme suit :
 - i. Pour Nom de la planification, spécifiez un nom descriptif pour la planification.
 - ii. Pour Fréquence et les champs associés, configurez l'intervalle entre les exécutions de stratégie.

Vous pouvez configurer les exécutions de politique selon une planification quotidienne, hebdomadaire, mensuelle ou annuelle. Vous pouvez également sélectionner Expression cron personnalisée pour spécifier un intervalle allant jusqu'à un an. Pour plus d'informations, consultez la section Expressions [cron et rate](#) dans le guide de l'EventBridge utilisateur Amazon.

 Note

Si vous devez activer l'archivage des instantanés pour la planification, vous devez sélectionner la fréquence mensuelle ou annuelle, ou vous devez spécifier une expression cron avec une fréquence de création d'au moins 28 jours.

Si vous spécifiez une fréquence mensuelle qui crée des instantanés un jour spécifique d'une semaine spécifique (par exemple, le deuxième jeudi du mois), alors pour une planification basée sur le nombre, le nombre de rétention du niveau d'archivage doit être de 4 ou plus.

- iii. Pour Démarrage à, spécifiez l'heure de démarrage planifiée des exécutions de la stratégie. La première exécution de politique commence dans l'heure qui suit l'heure programmée. L'heure doit être au format UTC hh:mm.
- iv. Pour Type de rétention, spécifiez la stratégie de rétention des instantanés créés par la planification.

Vous pouvez retenir les instantanés en fonction de leur nombre total ou de leur âge.

- **Count-based rétention**
 - Lorsque l'archivage des instantanés est désactivé, la plage s'étend de 1 à 1000. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage.
 - Lorsque l'archivage des instantanés est activé, la plage s'étend de 0 (archiver immédiatement après la création) à 1000. Une fois le seuil de rétention du niveau standard atteint, l'instantané est converti en instantané complet et est déplacé vers le niveau d'archivage.
- **Age-based rétention**
 - Lorsque l'archivage des instantanés est désactivé, la plage s'étend de 1 jour à 100 ans. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage.
 - Lorsque l'archivage des instantanés est activé, la plage s'étend de 0 jour (archivage immédiat après la création) à 100 ans. Une fois le seuil de rétention du niveau standard atteint, l'instantané est converti en instantané complet et est déplacé vers le niveau d'archivage.

 Note

- Toutes les planifications doivent avoir le même type de rétention (basé sur l'âge ou sur le nombre). Vous pouvez spécifier le type de conservation pour la planification 1 uniquement. Les planifications 2, 3 et 4 héritent du type de conservation de la planification 1. Chaque planification peut avoir son propre nombre ou sa propre période de conservation.
- Si vous activez la restauration rapide des instantanés, la copie inter-régions ou le partage d'instantanés, vous devez spécifier un nombre de rétention de 1 ou plus, ou une durée de conservation de 1 jour ou plus.

- v. (AWS Outposts et clients de la zone locale uniquement) Spécifiez la destination du cliché.

Pour Destination des instantanés, spécifiez la destination des instantanés créés par la politique.

- Si la politique cible les ressources d'une région, des instantanés doivent être créés dans la même région. AWS La région est sélectionnée pour vous.
 - Si la politique cible les ressources d'une zone locale, vous pouvez créer des instantanés dans la même zone locale que la ressource source ou dans sa région parente.
 - Si la politique cible des ressources sur une Outpost, vous pouvez créer des instantanés sur la même ressource Outpost que la source ou dans sa région mère.
- b. Configurez le balisage pour les instantanés.

Dans la section Etiquetage, procédez comme suit :

- i. Pour copier toutes les étiquettes définies par l'utilisateur à partir du volume source vers les instantanés créés par la planification, sélectionnez Copier les étiquettes à partir de la source.
 - ii. Pour spécifier des étiquettes supplémentaires à attribuer aux instantanés créés par cette planification, choisissez Ajouter des étiquettes.
- c. Configurez les scripts pré-scripts et les post-scripts pour des instantanés cohérents avec les applications.

Pour de plus amples informations, veuillez consulter [Automatisez les instantanés cohérents avec les applications avec Data Lifecycle Manager](#).

- d. (Politiques ciblant uniquement les volumes) Configurez l'archivage des instantanés.

Dans la section Archivage des instantanés, procédez comme suit :

 Note

Vous ne pouvez activer l'archivage des instantanés que pour une seule planification dans une politique.

- i. Pour activer l'archivage des instantanés pour la planification, sélectionnez Archive snapshots created by this schedule (Instantanés d'archives créés selon cette planification).

 Note

Vous pouvez activer l'archivage des instantanés uniquement si la fréquence de création des instantanés est mensuelle ou annuelle, ou si vous spécifiez une expression cron avec une fréquence de création d'au moins 28 jours.

- ii. Spécifiez la règle de rétention pour les instantanés dans le niveau d'archivage.
 - Pour les planifications basées sur le nombre, spécifiez le nombre d'instantanés à retenir dans le niveau d'archivage. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage. Par exemple, si vous spécifiez le chiffre 3, la planification retiendra un maximum de 3 instantanés dans le niveau d'archivage. Lorsque le quatrième instantané est archivé, le plus ancien des trois instantanés existants dans le niveau d'archivage est supprimé.
 - Pour les planifications basées sur l'âge, spécifiez la période pour laquelle il convient de retenir les instantanés dans le niveau d'archivage. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage. Par exemple, si vous spécifiez une période de 120 jours, la planification supprimera automatiquement les instantanés du niveau d'archivage lorsqu'ils atteignent cet âge.

 Important

La période de rétention minimale pour les instantanés archivés est de 90 jours. Vous devez spécifier une règle de rétention qui retient l'instantané pendant au moins 90 jours.

- e. Activez la restauration rapide des instantanés.

Pour activer la restauration rapide des instantanés créés par la planification, dans la section Restauration d'instantané rapide, sélectionnez Activer la restauration d'instantané rapide. Si vous activez la restauration d'instantané rapide, vous devez choisir les zones de disponibilité dans lesquelles le faire. Si la planification utilise une planification de rétention basée sur l'âge, vous devez spécifier la période pendant laquelle activer la restauration d'instantané rapide pour chaque instantané. Si la

planification utilise une rétention basée sur le nombre, vous devez spécifier le nombre maximum d'instantanés à activer pour la restauration d'instantané rapide.

Si le calendrier crée des instantanés sur un Outpost, vous ne pouvez pas activer la restauration rapide des instantanés. La restauration rapide des instantanés n'est pas prise en charge avec les instantanés locaux stockés sur un Outpost.

 Note

Vous êtes facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée pour un instantané dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure.

f. Configurez la copie entre régions.

Pour copier les instantanés créés par le calendrier vers une Outpost ou plusieurs régions, dans la section **Cross-Region Copie**, sélectionnez **Activer la copie entre régions**.

Si le calendrier crée des instantanés dans une région, vous pouvez copier les instantanés dans un maximum de trois régions supplémentaires ou Outposts dans votre compte. Vous devez spécifier une règle de copie entre régions distincte pour chaque région de destination ou Outpost.

Pour chaque région ou Outpost, vous pouvez choisir différentes politiques de conservation et choisir de copier toutes les balises ou de ne pas les copier. Si l'instantané source est chiffré ou si le chiffrement par défaut est activé, les instantanés copiés sont chiffrés. Si l'instantané source n'est pas chiffré, vous pouvez activer le chiffrement. Si vous ne spécifiez pas de clé KMS, les instantanés sont chiffrés à l'aide de la clé KMS par défaut pour le chiffrement EBS dans chaque région de destination. Si vous spécifiez une clé KMS pour la Région de destination, le rôle IAM sélectionné doit avoir accès à la clé KMS.

 Note

Vous devez vous assurer de ne pas dépasser le nombre de copies simultanées d'instantanés par région.

Si la politique crée des instantanés sur un Outpost, vous ne pouvez pas copier les instantanés vers une région ou vers une autre Outpost et les paramètres de copie entre régions ne sont pas disponibles.

g. Configurez le partage entre comptes.

Dans le Cross-account partage, configurez la politique pour partager automatiquement les instantanés créés par le calendrier avec d'autres AWS comptes. Procédez comme suit :

- i. Pour activer le partage avec d'autres AWS comptes, sélectionnez **Activer le partage entre comptes**.
- ii. Pour ajouter les comptes avec lesquels partager les instantanés, choisissez **Ajouter un compte**, entrez l'ID de compte AWS de 12 chiffres, puis choisissez **Ajouter**.
- iii. Pour annuler automatiquement le partage d'instantanés partagés après une période spécifique, sélectionnez **Unshare automatically (Annuler le partage automatiquement)**. Si vous choisissez d'annuler automatiquement le partage d'instantanés partagés, la période à l'issue de laquelle le partage est annulé ne peut pas être plus longue que la période pendant laquelle la politique retient ses instantanés. Par exemple, si la politique est configurée pour retenir les instantanés pendant 5 jours, vous pouvez configurer la politique de façon à ce qu'elle annule automatiquement le partage des instantanés partagés après jusqu'à 4 jours. Cela s'applique aux politiques avec des configurations de rétention d'instantanés basées sur l'âge et le nombre.

Si vous n'activez pas l'annulation automatique du partage, l'instantané est partagé jusqu'à sa suppression.

 Note

Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être partagés. Vous ne pouvez pas partager d'instantanés chiffrés à l'aide de la clé KMS de chiffrement EBS par défaut. Si vous partagez des instantanés chiffrés, vous devez également partager la clé KMS utilisée pour chiffrer le volume source avec les comptes cibles. Pour plus d'informations, consultez [Autoriser des utilisateurs d'autres comptes à](#)

[utiliser une clé KMS](#) dans le Guide du développeur AWS Key Management Service .

- h. Pour ajouter des planifications, choisissez l'option Ajouter une planification en haut de l'écran. Pour chaque planification supplémentaire, remplissez les champs comme décrit précédemment dans cette rubrique.
 - i. Après avoir ajouté les planifications requises, choisissez Examiner une stratégie.
12. Examinez le récapitulatif de la stratégie, puis choisissez Créer une stratégie.

 Note

Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consultez [Résoudre les problèmes liés à Amazon Data Lifecycle Manager](#) pour plus d'informations.

Command line

Utilisez la commande [create-lifecycle-policy](#) pour créer une stratégie de cycle de vie des instantanés. Pour `PolicyType`, spécifiez `EBS_SNAPSHOT_MANAGEMENT`.

 Note

Pour simplifier la syntaxe, les exemples suivants utilisent un fichier JSON, `policyDetails.json`, qui comportent les détails de la stratégie.

Exemple 1 — Politique de cycle de vie des instantanés avec deux planifications

Cet exemple montre comment créer une stratégie de cycle de vie des instantanés qui crée des instantanés de tous les volumes dont la clé de balise `costcenter` comporte une valeur de 115. La politique comprend deux planifications. La première planification crée un instantané tous les jours à 3h00 UTC. La deuxième planification crée un instantané hebdomadaire tous les vendredis à 17h00 UTC.

```
aws dlm create-lifecycle-policy \  
  --description "My volume policy" \  
  --policy-details policyDetails.json
```

```
--state ENABLED \  
--execution-role-arn  
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \  
--policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{  
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",  
  "ResourceTypes": [  
    "VOLUME"  
  ],  
  "TargetTags": [{  
    "Key": "costcenter",  
    "Value": "115"  
  }],  
  "Schedules": [{  
    "Name": "DailySnapshots",  
    "TagsToAdd": [{  
      "Key": "type",  
      "Value": "myDailySnapshot"  
    }],  
    "CreateRule": {  
      "Interval": 24,  
      "IntervalUnit": "HOURS",  
      "Times": [  
        "03:00"  
      ]  
    },  
    "RetainRule": {  
      "Count": 5  
    },  
    "CopyTags": false  
  },  
  {  
    "Name": "WeeklySnapshots",  
    "TagsToAdd": [{  
      "Key": "type",  
      "Value": "myWeeklySnapshot"  
    }],  
    "CreateRule": {  
      "CronExpression": "cron(0 17 ? * FRI *)"  
    }  
  },  
}
```

```

    "RetainRule": {
      "Count": 5
    },
    "CopyTags": false
  }
}]

```

Si la demande aboutit, la commande renvoie l’ID de la politique nouvellement créée. Voici un exemple de sortie.

```

{
  "PolicyId": "policy-0123456789abcdef0"
}

```

Exemple 2 : politique de cycle de vie des instantanés qui cible les instances et crée des instantanés d’un sous-ensemble de volumes de données (non racine)

Cet exemple crée une politique de cycle de vie des instantanés qui crée des ensembles d’instantanés multi-volumes à partir d’instances ayant l’identification code=production. La politique ne comprend qu’une seule planification. La planification ne crée pas d’instantanés des volumes de données ayant l’identification code=temp.

```

aws dlm create-lifecycle-policy \
  --description "My volume policy" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file://policyDetails.json

```

Voici un exemple du fichier policyDetails.json.

```

{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "code",
    "Value": "production"
  }],
}

```

```

    "Parameters": {
      "ExcludeDataVolumeTags": [{
        "Key": "code",
        "Value": "temp"
      }]
    },
    "Schedules": [{
      "Name": "DailySnapshots",
      "TagsToAdd": [{
        "Key": "type",
        "Value": "myDailySnapshot"
      }],
      "CreateRule": {
        "Interval": 24,
        "IntervalUnit": "HOURS",
        "Times": [
          "03:00"
        ]
      },
      "RetainRule": {
        "Count": 5
      },
      "CopyTags": false
    }
  ]
}

```

Si la demande aboutit, la commande renvoie l’ID de la politique nouvellement créée. Voici un exemple de sortie.

```

{
  "PolicyId": "policy-0123456789abcdef0"
}

```

Exemple 3 : Politique de cycle de vie des instantanés qui automatise les instantanés locaux de Outpost resources

Cet exemple crée une politique de cycle de vie des instantanés qui crée des instantanés des volumes marqués `team=dev` sur l'ensemble de vos Outposts données. La politique crée les instantanés sur les mêmes volumes Outposts que les volumes sources. La stratégie crée des instantanés toutes les 12 heures à partir de `00:00` UTC.

```
aws dlm create-lifecycle-policy \
```

```
--description "My local snapshot policy" \
--state ENABLED \
--execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
--policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": "VOLUME",
  "ResourceLocations": "OUTPOST",
  "TargetTags": [{
    "Key": "team",
    "Value": "dev"
  }],
  "Schedules": [{
    "Name": "on-site backup",
    "CreateRule": {
      "Interval": 12,
      "IntervalUnit": "HOURS",
      "Times": [
        "00:00"
      ],
    },
    "Location": [
      "OUTPOST_LOCAL"
    ],
    },
    "RetainRule": {
      "Count": 1
    },
    "CopyTags": false
  }
}]}
```

Exemple 4 : Politique de cycle de vie des instantanés qui crée des instantanés dans une région et les copie dans un Outpost

L'exemple de stratégie suivant crée des instantanés de volumes balisés avec `team=dev`. Les instantanés sont créés dans la même Région que le volume source. Les instantanés sont créés toutes les 12 heures à partir de `00:00` UTC et conservent un maximum d'1 instantané. La politique copie également les instantanés vers Outpost `arn:aws:outposts:us-`

east-1:123456789012:outpost/op-1234567890abcdef0, chiffre les instantanés copiés à l'aide de la clé de chiffrement KMS par défaut et conserve les copies pendant un mois. 1

```
aws dlm create-lifecycle-policy \
  --description "Copy snapshots to Outpost" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file:///policyDetails.json
```

Voici un exemple du fichier policyDetails.json.

```
{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": "VOLUME",
  "ResourceLocations": "CLOUD",
  "TargetTags": [{
    "Key": "team",
    "Value": "dev"
  }],
  "Schedules": [{
    "Name": "on-site backup",
    "CopyTags": false,
    "CreateRule": {
      "Interval": 12,
      "IntervalUnit": "HOURS",
      "Times": [
        "00:00"
      ],
      "Location": "CLOUD"
    },
    "RetainRule": {
      "Count": 1
    },
    "CrossRegionCopyRules" : [
      {
        "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
        "Encrypted": true,
        "CopyTags": true,
        "RetainRule": {
          "Interval": 1,
          "IntervalUnit": "MONTHS"
        }
      }
    ]
  }]
```

```

    }
  }]
}
[]

```

Exemple 5 – Politique de cycle de vie des instantanés avec une planification basée sur l'archivage et sur l'âge

Cet exemple montre comment créer une politique de cycle de vie des instantanés ciblant les volumes balisés avec Name=Prod. La politique comporte une planification basée sur l'âge qui crée des instantanés le premier jour de chaque mois à 9 h. La planification retient chaque instantané du niveau standard pendant un jour, après quoi elle les déplace vers le niveau d'archivage. Les instantanés sont stockés dans le niveau d'archivage pendant 90 jours avant d'être supprimés.

```

aws dlm create-lifecycle-policy \
  --description "Copy snapshots to Outpost" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file:///policyDetails.json

```

Voici un exemple du fichier policyDetails.json.

```

{
  "ResourceTypes": [ "VOLUME"],
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "Schedules" : [
    {
      "Name": "sched1",
      "TagsToAdd": [
        {"Key":"createdby","Value":"dlm"}
      ],
      "CreateRule": {
        "CronExpression": "cron(0 9 1 * ? *)"
      },
      "CopyTags": true,
      "RetainRule":{
        "Interval": 1,
        "IntervalUnit": "DAYS"
      },
      "ArchiveRule": {

```

```

        "RetainRule":{
            "RetentionArchiveTier": {
                "Interval": 90,
                "IntervalUnit": "DAYS"
            }
        }
    ],
    "TargetTags": [
        {
            "Key": "Name",
            "Value": "Prod"
        }
    ]
}

```

Exemple 6 – Politique de cycle de vie des instantanés avec une planification basée sur l'archivage et sur le nombre

Cet exemple montre comment créer une politique de cycle de vie des instantanés ciblant les volumes balisés avec `Purpose=Test`. La politique comporte une planification basée sur le nombre qui crée des instantanés le premier jour de chaque mois à 9 h. La planification archive les instantanés immédiatement après leur création et retient un maximum de trois instantanés dans le niveau d'archivage.

```

aws dlm create-lifecycle-policy \
  --description "Copy snapshots to Outpost" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file:///policyDetails.json

```

Voici un exemple du fichier `policyDetails.json`.

```

{
  "ResourceTypes": [ "VOLUME"],
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "Schedules" : [
    {
      "Name": "sched1",
      "TagsToAdd": [

```

```

        {"Key": "createdby", "Value": "dlm"}
    ],
    "CreateRule": {
        "CronExpression": "cron(0 9 1 * ? *)"
    },
    "CopyTags": true,
    "RetainRule": {
        "Count": 0
    },
    "ArchiveRule": {
        "RetainRule": {
            "RetentionArchiveTier": {
                "Count": 3
            }
        }
    }
},
],
"TargetTags": [
    {
        "Key": "Purpose",
        "Value": "Test"
    }
]
}

```

Considérations relatives aux stratégies de cycle de vie des instantanés

Les considérations générales suivantes s'appliquent aux politiques de cycle de vie des instantanés :

- Les politiques de cycle de vie des instantanés ciblent uniquement les instances ou les volumes qui se trouvent dans la même région que la politique.
- La première opération de création d'instantané démarre dans l'heure suivant l'heure de début spécifiée. Les opérations suivantes de création d'instantanés démarrent dans l'heure suivant leur heure planifiée.
- Vous pouvez créer plusieurs stratégies pour sauvegarder un volume ou une instance . Par exemple, si un volume EBS comporte deux identifications, l'identification A étant la cible de la politique A qui permet de créer un instantané toutes les 12 heures et l'identification B étant la cible de la politique B qui permet de créer un instantané toutes les 24 heures, Amazon Data Lifecycle Manager crée des instantanés en fonction des planifications des deux politiques. Vous

pouvez également obtenir le même résultat en créant une seule politique comportant plusieurs planifications. Par exemple, vous pouvez créer une politique unique qui cible uniquement la balise A et spécifier deux planifications : l'une pour toutes les 12 heures et l'autre pour toutes les 24 heures.

- Les balises de ressource cible sont sensibles à la casse.
- Si vous supprimez les balises cibles d'une ressource ciblée par une politique, Amazon Data Lifecycle Manager ne gère plus les instantanés existants dans le niveau standard et le niveau d'archivage. Vous devez les supprimer manuellement s'ils ne sont plus nécessaires.
- Si vous créez une politique qui cible des instances et que de nouveaux volumes sont attachés à l'instance après la création de la politique, les volumes nouvellement ajoutés sont inclus dans la sauvegarde lors de la prochaine exécution de la politique. Tous les volumes attachés à l'instance au moment de l'exécution de la politique sont inclus.
- Si une politique avec une planification personnalisée basée sur les crons est configurée pour créer un seul instantané, la politique ne supprime pas automatiquement cet instantané lorsque le seuil de rétention est atteint. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.
- Si vous créez une politique basée sur l'âge dans laquelle la période de conservation est plus courte que la fréquence de création, Amazon Data Lifecycle Manager conservera toujours le dernier instantané jusqu'à la création du suivant. Par exemple, si une politique basée sur l'âge crée un instantané par mois avec une période de conservation de sept jours, Amazon Data Lifecycle Manager conservera chaque pendant un mois, même si la période de conservation est de sept jours.

Les considérations suivantes s'appliquent à l'[archivage des instantanés](#) :

- Vous pouvez activer l'archivage des instantanés uniquement pour les politiques d'instantanés qui ciblent les volumes
- Vous ne pouvez spécifier une règle d'archivage que pour une seule planification par politique.
- Si vous utilisez la console, vous pouvez activer l'archivage des instantanés uniquement si la planification possède une fréquence de création mensuelle ou annuelle, ou si elle possède une expression cron avec une fréquence de création d'au moins 28 jours.

Si vous utilisez l' AWS API ou le AWS CLI AWS SDK, vous ne pouvez activer l'archivage des instantanés que si le calendrier comporte une expression cron avec une fréquence de création d'au moins 28 jours.

- La période de rétention minimale dans le niveau d'archivage est de 90 jours.

- Lorsqu'un instantané est archivé, il est converti en instantané complet lorsqu'il est déplacé vers le niveau d'archivage. Cela peut entraîner des coûts de stockage d'instantanés plus élevés. Pour de plus amples informations, veuillez consulter [Tarification et facturation pour l'archivage des instantanés Amazon EBS](#).
- La restauration rapide d'instantané et le partage d'instantanés sont désactivés pour les instantanés lorsqu'ils sont archivés.
- Si, dans le cas d'une année bissextile, votre règle de rétention résulte en une période de rétention d'archivage inférieure à 90 jours, Amazon Data Lifecycle Manager garantit la rétention des instantanés pendant la période minimale de 90 jours.
- Si vous archivez manuellement un instantané créé par Amazon Data Lifecycle Manager et que l'instantané est toujours archivé lorsque le seuil de rétention de la planification est atteint, Amazon Data Lifecycle Manager ne gère plus cet instantané. Toutefois, si vous restaurez l'instantané au niveau standard avant que le seuil de rétention de la planification ne soit atteint, la planification continuera à gérer l'instantané conformément aux règles de rétention.
- Si vous restaurez de façon permanente ou temporaire un instantané archivé par Amazon Data Lifecycle Manager et que l'instantané se trouve toujours dans le niveau standard lorsque le seuil de rétention de la planification est atteint, Amazon Data Lifecycle Manager ne gère plus l'instantané. Toutefois, si vous réarchivez l'instantané avant que le seuil de rétention de la planification soit atteint, la planification supprime l'instantané lorsque le seuil de rétention est atteint.
- Les instantanés archivés par Amazon Data Lifecycle Manager sont comptabilisés dans vos quotas `Archived snapshots per volume` et `In-progress snapshot archives per account`.
- Si une planification ne parvient pas à archiver un instantané après de nouvelles tentatives pendant 24 heures, l'instantané reste au niveau standard et sa suppression est planifiée en fonction de l'heure à laquelle il aurait été supprimé du niveau d'archivage. Par exemple, si la planification archive les instantanés pendant 120 jours, ceux-ci restent au niveau standard pendant 120 jours après l'échec de l'archivage avant d'être supprimés définitivement. Pour les planifications basées sur le nombre, l'instantané n'est pas comptabilisé dans le nombre de rétention de la planification.
- Les instantanés doivent être archivés dans la région dans laquelle ils ont été créés. Si vous avez activé la copie inter-régions et l'archivage des instantanés, Amazon Data Lifecycle Manager n'archive pas la copie d'instantané.
- Les instantanés archivés par Amazon Data Lifecycle Manager sont balisés avec la balise système `aws:dlm:archived=true`. De plus, les instantanés créés par une planification basée sur l'archivage et sur l'âge sont balisés avec la balise système `aws:dlm:expirationTime`, qui indique la date et l'heure auxquelles l'archivage de l'instantané est prévu.

Les considérations suivantes s'appliquent à l'exclusion des volumes racine et des volumes de données (non racine) :

- Si vous choisissez d'exclure les volumes de démarrage et que vous spécifiez des balises qui excluent par conséquent tous les volumes de données supplémentaires attachés à une instance, Amazon Data Lifecycle Manager ne créera aucun instantané pour l'instance concernée et émettra une `SnapshotsCreateFailed` CloudWatch métrique. Pour de plus amples informations, veuillez consulter [Surveillez les politiques à l'aide CloudWatch](#).

Les considérations suivantes s'appliquent à la suppression de volumes ou à la résiliation d'instances ciblées par les politiques de cycle de vie des instantanés :

- Si vous supprimez un volume ou résiliez une instance ciblée par une politique avec une planification de rétention basée sur le nombre, Amazon Data Lifecycle Manager ne gère plus les instantanés dans le niveau standard et le niveau d'archivage créés à partir du volume supprimé ou de l'instance résiliée. Vous devez supprimer ces instantanés précédents manuellement lorsqu'ils ne sont plus nécessaires.
- Si vous supprimez un volume ou résiliez une instance ciblée par une politique avec une planification de rétention basée sur l'âge, la politique continue de supprimer les instantanés du niveau standard et du niveau d'archivage créés à partir du volume supprimé ou de l'instance résiliée selon la planification définie, jusqu'au dernier instantané, mais sans l'inclure. Vous devez supprimer manuellement le dernier instantané s'il n'est plus nécessaire.

Les considérations suivantes s'appliquent aux politiques de cycle de vie des instantanés et [à la restauration d'instantané rapide](#) :

- Amazon Data Lifecycle Manager peut activer la restauration rapide des instantanés uniquement pour les instantanés d'une taille inférieure ou égale à 16 TiO. Pour de plus amples informations, veuillez consulter [Restauration d'instantané rapide Amazon EBS](#).
- Un instantané qui est activé pour la restauration d'instantané rapide reste activé, même si vous supprimez ou désactivez la politique, si vous désactivez la restauration d'instantané rapide pour la politique ou si vous désactivez la restauration d'instantané rapide pour la zone de disponibilité. Vous devez désactiver manuellement la restauration d'instantané rapide pour ces instantanés.
- Si vous activez la restauration d'instantané rapide pour une politique et que vous dépassez le nombre maximum d'instantanés pouvant être activés pour la restauration d'instantané rapide, Amazon Data Lifecycle Manager crée des instantanés comme prévu, mais ne les active pas pour la

restauration d'instantané rapide. Une fois qu'un instantané activé pour la restauration d'instantané rapide est supprimé, l'instantané suivant créé par Amazon Data Lifecycle Manager est activé pour la restauration rapide d'instantané.

- Lorsque la restauration d'instantané rapide pour un instantané, l'optimisation de ce dernier dure 60 minutes par Tio. Nous vous recommandons de configurer vos planifications de stratégie qui assurent l'optimisation complète de chaque instantané avant que Amazon Data Lifecycle Manager ne crée l'instantané suivant.
- Si vous activez la restauration rapide des instantanés pour une stratégie ciblant les instances, Amazon Data Lifecycle Manager permet une restauration rapide des instantanés pour chaque instantané du cliché multivolume défini individuellement. Si Amazon Data Lifecycle Manager ne parvient pas à activer la restauration rapide des instantanés pour l'un des instantanés du jeu d'instantanés multi-volumes, il tentera toujours d'activer la restauration rapide des instantanés pour les instantanés restants du jeu de d'instantanés.
- Vous êtes facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée pour un instantané dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure. Pour plus d'informations, consultez [Tarification et facturation](#).

 Note

Selon la configuration de vos politiques de cycle de vie, plusieurs instantanés peuvent être activés pour une restauration rapide dans de multiples zones de disponibilité en simultanée.

Les considérations suivantes s'appliquent aux politiques de cycle de vie des snapshots et [Multi-Attach](#) aux volumes activés :

- Lors de la création d'une politique de cycle de vie qui cible les instances ayant le même volume Multi-Attach activé, Amazon Data Lifecycle Manager crée un instantané du volume pour chaque instance attachée. Utilisez la balise timestamp pour identifier l'ensemble d'instantanés temporels créés à partir des instances attachées.

Les considérations suivantes s'appliquent au partage des instantanés entre comptes :

- Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être partagés.

- Vous ne pouvez pas partager d'instantanés chiffrés à l'aide de la clé KMS de chiffrement EBS par défaut.
- Si vous partagez des instantanés chiffrés, vous devez également partager la clé KMS utilisée pour chiffrer le volume source avec les comptes cibles. Pour plus d'informations, consultez [Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS](#) dans le Guide du développeur AWS Key Management Service .

Les considérations suivantes s'appliquent aux politiques des instantanés et à [l'archivage des instantanés](#) :

- Si vous archivez manuellement un instantané créé par une politique et que cet instantané se trouve dans le niveau d'archivage lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager ne supprime pas l'instantané. Amazon Data Lifecycle Manager ne gère pas les instantanés lorsqu'ils sont stockés dans le niveau d'archivage. Si vous n'avez plus besoin des instantanés qui sont stockés dans le niveau d'archivage, vous devez les supprimer manuellement.

Les considérations suivantes s'appliquent aux politiques relatives aux captures instantanées et à la [corbeille](#) :

- Si Amazon Data Lifecycle Manager supprime un instantané et l'envoie à la corbeille lorsque le seuil de rétention de la politique est atteint, et que vous restaurez manuellement l'instantané à partir de la corbeille, vous devez supprimer manuellement cet instantané s'il n'est plus nécessaire. Amazon Data Lifecycle Manager ne gèrera plus l'instantané.
- Si vous supprimez manuellement un instantané créé par une politique et que cet instantané se trouve dans la corbeille lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager ne supprime pas l'instantané. Amazon Data Lifecycle Manager ne gère pas les instantanés lorsqu'ils sont stockés dans la corbeille.

Si l'instantané est restauré à partir de la corbeille avant que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager supprime l'instantané lorsque le seuil de rétention de la politique est atteint.

Si l'instantané est restauré à partir de la corbeille après que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager ne supprime plus l'instantané. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Les considérations suivantes s'appliquent aux politiques de cycle de vie des instantanés qui sont dans l'état d'erreur :

- Pour les politiques avec des planifications de rétention basées sur l'âge, les instantanés qui sont configurés pour expirer alors que la politique est dans l'état `error` sont conservés indéfiniment. Vous devez supprimer les instantanés manuellement. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la suppression des instantanés à mesure que leurs périodes de rétention expirent.
- Pour les politiques avec des planifications de rétention basée sur le nombre, la politique arrête de créer et de supprimer des instantanés pendant qu'elle est dans l'état `error`. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la création d'instantanés, ainsi que la suppression d'instantanés lorsque le seuil de rétention est atteint.

Les considérations suivantes s'appliquent aux politiques d'instantanés et au [verrouillage d'instantanés](#) :

- Si vous verrouillez manuellement un instantané créé par Amazon Data Lifecycle Manager et que l'instantané est toujours verrouillé lorsque son seuil de conservation est atteint, Amazon Data Lifecycle Manager ne gère plus cet instantané. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.
- Si vous verrouillez manuellement un instantané qui a été créé par Amazon Data Lifecycle Manager avec la restauration rapide activée et que l'instantané est toujours verrouillé lorsque son seuil de conservation est atteint, Amazon Data Lifecycle Manager ne désactive pas la restauration rapide de l'instantané et ne supprime pas l'instantané. Vous devez désactiver la restauration d'instantané rapide et supprimer manuellement l'instantané s'il n'est plus nécessaire.
- Si vous inscrivez manuellement un instantané qui a été créé par Amazon Data Lifecycle Manager avec une AMI puis que vous verrouillez cet instantané, et que l'instantané est toujours verrouillé et associé à l'AMI lorsque son seuil de conservation est atteint, Amazon Data Lifecycle Manager continue de tenter de supprimer l'instantané. Lorsque l'inscription de l'AMI est annulée et que l'instantané est déverrouillé, Amazon Data Lifecycle Manager supprime automatiquement l'instantané.

Ressources supplémentaires

Pour plus d'informations, consultez le blog [Automatiser la gestion des snapshots Amazon EBS et des AMI à l'aide du](#) AWS stockage Amazon Data Lifecycle Manager.

Automatisez les instantanés cohérents avec les applications avec Data Lifecycle Manager

Vous pouvez automatiser les instantanés cohérents par rapport à l'application avec Amazon Data Lifecycle Manager en activant les pré-scripts et les post-scripts dans vos politiques de cycle de vie des instantanés qui ciblent les instances.

Amazon Data Lifecycle Manager s'intègre à AWS Systems Manager (Systems Manager) pour prendre en charge des instantanés cohérents avec les applications. Amazon Data Lifecycle Manager utilise les documents de commande Systems Manager (SSM) qui incluent des pré-scripts et des post-scripts pour automatiser les actions nécessaires pour créer des instantanés cohérents par rapport à l'application. Avant qu'Amazon Data Lifecycle Manager ne lance la création d'un instantané, il exécute les commandes du pré-script pour geler et vider I/O. Une fois qu'Amazon Data Lifecycle Manager a lancé la création d'un instantané, il exécute les commandes du post-script pour I/O dégeler.

Avec Amazon Data Lifecycle Manager, vous pouvez automatiser les instantanés cohérents par rapport à l'application pour les applications suivantes :

- applications Windows avec Volume Shadow Copy Service (VSS) ;
- SAP HANA à l'aide d'un document SSDM AWS géré. pour plus d'informations, consultez [Amazon EBS snapshots for SAP HANA](#).
- Self-managed bases de données, telles que MySQL, PostgreSQL ou InterSystems IRIS, à l'aide de modèles de documents SSM

Rubriques

- [Exigences relatives à l'utilisation des pré-scripts et post-scripts](#)
- [Démarrage avec les instantanés cohérents par rapport à l'application](#)
- [Considérations relatives aux sauvegardes VSS avec Amazon Data Lifecycle Manager](#)
- [Responsabilité partagée pour les instantanés cohérents par rapport à l'application](#)

Exigences relatives à l'utilisation des pré-scripts et post-scripts

Le tableau suivant décrit les exigences relatives à l'utilisation des pré-scripts et des post-scripts avec Amazon Data Lifecycle Manager.

Application-consistent instantanés

Exigence	Sauvegarde VSS	Document SSM personnalisé	Autres cas d'utilisation
L'agent SSM est installé et s'exécute sur les instances cibles	✓	✓	✓
Configuration requise pour le système VSS satisfaite sur les instances cibles	✓		
Profil d'instance compatible VSS associé aux instances cibles	✓		
Composants VSS installés sur les instances cibles	✓		
Préparer un document SSM à l'aide de commandes de pré-script et de post-script		✓	✓
Préparer le rôle IAM d'Amazon Data Lifecycle Manager, exécuter les pré-scripts et les post-scripts	✓	✓	✓
Créez une politique de capture instantanée qui cible les instances et qui est	✓	✓	✓

Application-consistent instantanés

configurée pour les
pré-scripts et les post-
scripts

Démarrage avec les instantanés cohérents par rapport à l'application

Cette section explique les étapes à suivre pour automatiser les instantanés cohérents par rapport à l'application à l'aide d'Amazon Data Lifecycle Manager.

Étape 1 : Préparer les instances cibles

Vous devez préparer les instances ciblées pour les instantanés cohérents par rapport à l'application à l'aide d'Amazon Data Lifecycle Manager. Effectuez l'une des actions suivantes en fonction de votre cas d'utilisation.

Prepare for VSS Backups

Pour préparer vos instances cibles pour les sauvegardes VSS

1. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.

Pour plus d'informations, consultez la section [Utilisation de l'agent SSM sur les instances EC2 pour Windows Server](#).

2. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez [Vérification du statut de l'SSM Agent et démarrage de l'agent](#).
3. Configurez Systems Manager pour des instances Amazon EC2. Pour plus d'informations, consultez [Configuration de Systems Manager pour des instances Amazon EC2](#) dans le Guide de l'utilisateur AWS Systems Manager .
4. [Assurez-vous que la configuration requise pour les sauvegardes VSS est respectée.](#)
5. [Associez un profil d' VSS-enabled instance aux instances cibles.](#)
6. [Installez les composants VSS.](#)

Prepare for SAP HANA backups

Pour préparer vos instances cibles pour les sauvegardes SAP HANA

1. Préparez l'environnement SAP HANA sur vos instances cibles.
 - a. Configurez votre instance avec SAP HANA. Si vous ne possédez pas encore d'environnement SAP HANA, vous pouvez consulter la rubrique [SAP HANA Environment Setup on AWS](#).
 - b. Connectez-vous à SystemDB en tant qu'utilisateur administrateur approprié.
 - c. Créez un utilisateur de sauvegarde de base de données à utiliser avec Amazon Data Lifecycle Manager.

```
CREATE USER username PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

Par exemple, la commande suivante crée un utilisateur nommé `d1m_user` avec le mot de passe `password`.

```
CREATE USER d1m_user PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

- d. Attribuez le rôle `BACKUP_OPERATOR` à l'utilisateur de sauvegarde de base de données que vous avez créé à l'étape précédente.

```
GRANT BACKUP_OPERATOR TO username
```

Par exemple, la commande suivante attribue le rôle à un utilisateur nommé `d1m_user`.

```
GRANT BACKUP_OPERATOR TO d1m_user
```

- e. Connectez-vous au système d'exploitation en tant qu'administrateur, par exemple `sidadm`.
 - f. Créez une entrée `hdbuserstore` pour stocker les informations de connexion afin que le document SSM SAP HANA puisse se connecter à SAP HANA sans que les utilisateurs aient à saisir ces informations.

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER  
localhost:3hana_instance_number13 username password
```

Par exemple :

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER localhost:30013 dlm_user password
```

g. Testez la connexion.

```
hdbsql -U DLM_HANADB_SNAPSHOT_USER "select * from dummy"
```

2. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.

Pour plus d'informations, consultez la section Installation [manuelle de l'agent SSM sur les instances EC2 pour Linux](#).

3. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez [Vérification du statut de l'SSM Agent et démarrage de l'agent](#).
4. Configurez Systems Manager pour des instances Amazon EC2. Pour plus d'informations, consultez [Configuration de Systems Manager pour des instances Amazon EC2](#) dans le Guide de l'utilisateur AWS Systems Manager .

Prepare for custom SSM documents

Pour préparer les documents SSM personnalisés de vos instances cibles

1. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.
 - (instances Linux) Installation [manuelle de l'agent SSM sur des instances EC2 pour Linux](#)
 - (instances Windows) [Utilisation de l'agent SSM sur les instances EC2 pour Windows Server](#)
2. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez [Vérification du statut de l'SSM Agent et démarrage de l'agent](#).
3. Configurez Systems Manager pour des instances Amazon EC2. Pour plus d'informations, consultez [Configuration de Systems Manager pour des instances Amazon EC2](#) dans le Guide de l'utilisateur AWS Systems Manager .

Étape 2 : Préparer le document SSM

Note

Cette étape est requise uniquement pour les documents SSM personnalisés. Elle n'est pas nécessaire pour les sauvegardes VSS ou SAP HANA. Pour VSS Backups et SAP HANA, Amazon Data Lifecycle Manager utilise le document SSM AWS géré.

Si vous automatisez des instantanés cohérents avec les applications pour une base de données autogérée, telle que MySQL, PostgreSQL ou InterSystems IRIS, vous devez créer un document de commande SSM qui inclut un pré-script pour geler et vider I/O avant le lancement de la création de l'instantané, et un post-script pour le décongeler après le lancement de la création du cliché. I/O

Si votre base de données MySQL, PostgreSQL ou InterSystems IRIS utilise des configurations standard, vous pouvez créer un document de commande SSM à l'aide de l'exemple de contenu du document SSM ci-dessous. Si votre base de données MySQL, PostgreSQL ou InterSystems IRIS utilise une configuration non standard, vous pouvez utiliser l'exemple de contenu ci-dessous comme point de départ pour votre document de commande SSM, puis le personnaliser en fonction de vos besoins. Si vous souhaitez créer un nouveau document SSM à partir de zéro, vous pouvez également utiliser le modèle de document SSM vide ci-dessous et ajouter vos commandes pré et post dans les sections de document appropriées.

Notez ce qui suit :

- Il est de votre responsabilité de vous assurer que le document SSM exécute les actions correctes et requises pour la configuration de votre base de données.
- La cohérence des instantanés avec les applications est garantie uniquement si les scripts pré et post de votre document SSM peuvent être gelés, vidés et dégelés avec succès. I/O
- Le document SSM doit inclure les champs obligatoires pour `allowedValues`, notamment `pre-script`, `post-script` et `dry-run`. Amazon Data Lifecycle Manager exécutera des commandes sur votre instance en fonction du contenu de ces sections. Si votre document SSM ne contient pas ces sections, Amazon Data Lifecycle Manager le considérera comme un échec d'exécution.

MySQL sample document content

```

###=====###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
# this
# software and associated documentation files (the "Software"), to deal in the
# Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for MySQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
    and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12})$
  command:
    # Data Lifecycle Manager will trigger the pre-script and post-script actions
    during policy execution.
    # 'dry-run' option is intended for validating the document execution without
    triggering any commands
    # on the instance. The following allowedValues will allow Data Lifecycle Manager
    to successfully
    # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
    be executed.
    allowedValues:

```

- pre-script
- post-script
- dry-run

mainSteps:

- action: aws:runShellScript
 - description: Run MySQL Database freeze/thaw commands
 - name: run_pre_post_scripts
 - precondition:
 - StringEquals:
 - platformType
 - Linux
 - inputs:
 - runCommand:
 - |
 - #!/bin/bash

###=====###

Error Codes

###=====###

The following Error codes will inform Data Lifecycle Manager of the type of error

and help guide handling of the error.

The Error code will also be emitted via AWS Eventbridge events in the 'cause' field.

1 Pre-script failed during execution - 201

2 Post-script failed during execution - 202

3 Auto thaw occurred before post-script was initiated - 203

4 Pre-script initiated while post-script was expected - 204

5 Post-script initiated while pre-script was expected - 205

6 Application not ready for pre or post-script initiation - 206

###=====###

Global variables

###=====###

START=\$(date +%s)

For testing this script locally, replace the below with OPERATION=\$1.

OPERATION={{ command }}

FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'

FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'

FS_BUSY_ERROR='mount point is busy'

```
# Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
# duration specified in the global variable below. Choose the duration based
on your
# database application's tolerance to freeze.
export AUTO_THAW_DURATION_SECS="60"

# Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"
    # Check if filesystem is already frozen. No error code indicates that
filesystem
# is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
    check_fs_freeze
    # Execute the DB commands to flush the DB in preparation for snapshot
snap_db
    # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
    freeze_fs

    echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
    $(nohup bash -c execute_schedule_auto_thaw >/dev/null 2>&1 &)
}

# Add all post-script actions to be performed within the function below
execute_post_script() {
    echo "INFO: Start execution of post-script"
    # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen.
    unfreeze_fs
    thaw_db
}

# Execute Auto Thaw to automatically unfreeze the application after the
duration configured
# in the AUTO_THAW_DURATION_SECS global variable.
execute_schedule_auto_thaw() {
    sleep ${AUTO_THAW_DURATION_SECS}
    execute_post_script
}

# Disable Auto Thaw if it is still enabled
```

```

    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == */boot* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                fi
            fi
            exit 204
        fi
    }

```

```

        # If the check filesystem freeze failed due to any reason other
        than the filesystem already frozen, return 201
        echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
        to error - $errormessage"
        exit 201
    fi
done

}

# Iterate over all the mountpoints and freeze the filesystem.
freeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)
    do
        # Freeze of the root and boot filesystems is dangerous. Hence, skip
        filesystem freeze
        # operations for root and boot mountpoints.
        if [ $target == '/' ]; then continue; fi
        if [[ "$target" == */boot* ]]; then continue; fi
        echo "INFO: Freezing $target"
        error_message=$(sudo fsfreeze -f $target 2>&1)
        if [ $? -ne 0 ];then
            # If the filesystem is already in frozen, return error code 204
            if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                echo "ERROR: Filesystem ${target} already frozen. Return Error
                Code: 204"
                sudo mysql -e 'UNLOCK TABLES;'
                exit 204
            fi
            # If the filesystem freeze failed due to any reason other than the
            filesystem already frozen, return 201
            echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
            $errormessage"
            thaw_db
            exit 201
        fi
        echo "INFO: Freezing complete on $target"
    done
}

# Iterate over all the mountpoints and unfreeze the filesystem.
unfreeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)
    do

```

```

        # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
        # Hence, will skip the root and boot mountpoints during unfreeze as
well.

        if [ $target == '/' ]; then continue; fi
        if [[ "$target" == */boot* ]]; then continue; fi
        echo "INFO: Thawing $target"
        error_message=$(sudo fsfreeze -u $target 2>&1)
        # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
        if [ $? -ne 0 ]; then
            if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                exit 205
            fi
            # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
            echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
            exit 202
        fi
        echo "INFO: Thaw complete on $target"
    done
}

snap_db() {
    # Run the flush command only when MySQL DB service is up and running
    sudo systemctl is-active --quiet mysqld.service
    if [ $? -eq 0 ]; then
        echo "INFO: Execute MySQL Flush and Lock command."
        sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
        # If the MySQL Flush and Lock command did not succeed, return error
code 201 to indicate pre-script failure
        if [ $? -ne 0 ]; then
            echo "ERROR: MySQL FLUSH TABLES WITH READ LOCK command failed."
            exit 201
        fi
        sync
    else
        echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Flush and Lock command."
    fi
}

```

```

thaw_db() {
    # Run the unlock command only when MySQL DB service is up and running
    sudo systemctl is-active --quiet mysqld.service
    if [ $? -eq 0 ]; then
        echo "INFO: Execute MySQL Unlock"
        sudo mysql -e 'UNLOCK TABLES;'
    else
        echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Unlock command."
    fi
}

export -f execute_schedule_auto_thaw
export -f execute_post_script
export -f unfreeze_fs
export -f thaw_db

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        execute_disable_auto_thaw
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time

```

```
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."
```

PostgreSQL sample document content

```
###=====###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
# this
# software and associated documentation files (the "Software"), to deal in the
# Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for PostgreSQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
    and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
    {4}-[a-fA-F0-9]{12})$
  command:
    # Data Lifecycle Manager will trigger the pre-script and post-script actions
    during policy execution.
    # 'dry-run' option is intended for validating the document execution without
    triggering any commands
    # on the instance. The following allowedValues will allow Data Lifecycle Manager
    to successfully
    # trigger pre and post script actions.
    type: String
```



```

    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
be executed.
    allowedValues:
      - pre-script
      - post-script
      - dry-run

```

```

mainSteps:
- action: aws:runShellScript
  description: Run PostgreSQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
      - platformType
      - Linux
  inputs:
    runCommand:
      - |
        #!/bin/bash

```

```

###=====###

```

```

    ### Error Codes

```

```

###=====###

```

```

    # The following Error codes will inform Data Lifecycle Manager of the type of
error

```

```

    # and help guide handling of the error.

```

```

    # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.

```

```

    # 1 Pre-script failed during execution - 201

```

```

    # 2 Post-script failed during execution - 202

```

```

    # 3 Auto thaw occurred before post-script was initiated - 203

```

```

    # 4 Pre-script initiated while post-script was expected - 204

```

```

    # 5 Post-script initiated while pre-script was expected - 205

```

```

    # 6 Application not ready for pre or post-script initiation - 206

```

```

###=====###

```

```

    ### Global variables

```

```

###=====###

```

```

    START=$(date +%s)

```

```

OPERATION={{ command }}
FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
FS_BUSY_ERROR='mount point is busy'

# Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
# duration specified in the global variable below. Choose the duration based
on your
# database application's tolerance to freeze.
export AUTO_THAW_DURATION_SECS="60"

# Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"
    # Check if filesystem is already frozen. No error code indicates that
filesystem
# is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
check_fs_freeze
# Execute the DB commands to flush the DB in preparation for snapshot
snap_db
# Freeze the filesystem. No error code indicates that filesystem was
succesfully frozen
freeze_fs

    echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
    $(nohup bash -c execute_schedule_auto_thaw >/dev/null 2>&1 &)
}

# Add all post-script actions to be performed within the function below
execute_post_script() {
    echo "INFO: Start execution of post-script"
    # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen
unfreeze_fs
}

# Execute Auto Thaw to automatically unfreeze the application after the
duration configured
# in the AUTO_THAW_DURATION_SECS global variable.
execute_schedule_auto_thaw() {
    sleep ${AUTO_THAW_DURATION_SECS}

```

```

        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == */boot* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then

```

```

        echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
        exit 204
    fi
    # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
    echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
    exit 201
fi
done
}

# Iterate over all the mountpoints and freeze the filesystem.
freeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)
    do
        # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
        # operations for root and boot mountpoints.
        if [ $target == '/' ]; then continue; fi
        if [[ "$target" == */boot* ]]; then continue; fi
        echo "INFO: Freezing $target"
        error_message=$(sudo fsfreeze -f $target 2>&1)
        if [ $? -ne 0 ];then
            # If the filesystem is already in frozen, return error code 204
            if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                exit 204
            fi
            # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
            echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
            exit 201
        fi
        echo "INFO: Freezing complete on $target"
    done
}

# Iterate over all the mountpoints and unfreeze the filesystem.
unfreeze_fs() {
    for target in $(lsblk -nlo MOUNTPOINTS)

```

```

do
    # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
    # Hence, will skip the root and boot mountpoints during unfreeze as
well.

    if [ $target == '/' ]; then continue; fi
    if [[ "$target" == */boot* ]]; then continue; fi
    echo "INFO: Thawing $target"
    error_message=$(sudo fsfreeze -u $target 2>&1)
    # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
    if [ $? -ne 0 ]; then
        if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
            echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
            exit 205
        fi
        # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
        echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
        exit 202
    fi
    echo "INFO: Thaw complete on $target"
done
}

snap_db() {
    # Run the flush command only when PostgreSQL DB service is up and running
sudo systemctl is-active --quiet postgresql
    if [ $? -eq 0 ]; then
        echo "INFO: Execute Postgres CHECKPOINT"
        # PostgreSQL command to flush the transactions in memory to disk
        sudo -u postgres psql -c 'CHECKPOINT;'
        # If the PostgreSQL Command did not succeed, return error code 201 to
indicate pre-script failure
        if [ $? -ne 0 ]; then
            echo "ERROR: Postgres CHECKPOINT command failed."
            exit 201
        fi
        sync
    else
        echo "INFO: PostgreSQL service is inactive. Skipping execution of
CHECKPOINT command."
    fi
}

```

```

    fi
}

export -f execute_schedule_auto_thaw
export -f execute_post_script
export -f unfreeze_fs

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        execute_disable_auto_thaw
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."

```

InterSystems IRIS sample document content

```

###=====###
# MIT License
#
# Copyright (c) 2024 InterSystems
#

```

```

# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in all
# copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
###=====###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
  feature for InterSystems IRIS.
parameters:
  executionId:
    type: String
    default: None
    description: Specifies the unique identifier associated with a pre and/or post
  execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12})$
  command:
    type: String
    # Data Lifecycle Manager will trigger the pre-script and post-script actions.
    You can also use this SSM document with 'dry-run' for manual testing purposes.
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
  be executed.
    #The following allowedValues will allow Data Lifecycle Manager to successfully
  trigger pre and post script actions.
    allowedValues:
      - pre-script
      - post-script
      - dry-run

mainSteps:

```

```

- action: aws:runShellScript
  description: Run InterSystems IRIS Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
      - platformType
      - Linux
  inputs:
    runCommand:
      - |
        #!/bin/bash

###=====###
    ### Global variables

###=====###
    DOCKER_NAME=iris
    LOGDIR=./
    EXIT_CODE=0
    OPERATION={{ command }}
    START=$(date +%s)

    # Check if Docker is installed
    # By default if Docker is present, script assumes that InterSystems IRIS is
running in Docker
    # Leave only the else block DOCKER_EXEC line, if you run InterSystems IRIS
non-containerised (and Docker is present).
    # Script assumes irissys user has OS auth enabled, change the OS user or
supply login/password depending on your configuration.
    if command -v docker &> /dev/null
    then
        DOCKER_EXEC="docker exec $DOCKER_NAME"
    else
        DOCKER_EXEC="sudo -i -u irissys"
    fi

    # Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"

    # find all iris running instances
    iris_instances=$(($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
'^up' | cut -c5- | awk '{print $1}')
```



```

echo "`date`: Running iris instances $iris_instances"

# Only for running instances
for INST in $iris_instances; do

    echo "`date`: Attempting to freeze $INST"

    # Detailed instances specific log
    LOGFILE=$LOGDIR/$INST-pre_post.log

    #check Freeze status before starting
    $DOCKER_EXEC irissession $INST -U '%SYS'
    "##Class(Backup.General).IsWDSuspendedExt()"
    freeze_status=$?
    if [ $freeze_status -eq 5 ]; then
        echo "`date`: ERROR: $INST IS already FROZEN"
        EXIT_CODE=204
    else
        echo "`date`: $INST is not frozen"
        # Freeze
        # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
        $DOCKER_EXEC irissession $INST -U '%SYS'
        "##Class(Backup.General).ExternalFreeze(\"$LOGFILE\",,,,,,600,,,300)"
        status=$?

        case $status in
            5) echo "`date`: $INST IS FROZEN"
                ;;
            3) echo "`date`: $INST FREEZE FAILED"
                EXIT_CODE=201
                ;;
            *) echo "`date`: ERROR: Unknown status code: $status"
                EXIT_CODE=201
                ;;
        esac
        echo "`date`: Completed freeze of $INST"
    fi
done
echo "`date`: Pre freeze script finished"
}

# Add all post-script actions to be performed within the function below
execute_post_script() {

```

```

echo "INFO: Start execution of post-script"

# find all iris running instances
iris_instances=$(($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
'^up' | cut -c5- | awk '{print $1}'))
echo "`date`: Running iris instances $iris_instances"

# Only for running instances
for INST in $iris_instances; do

    echo "`date`: Attempting to thaw $INST"

    # Detailed instances specific log
    LOGFILE=$LOGDIR/$INST-pre_post.log

    #check Freeze status befor starting
    $DOCKER_EXEC irissession $INST -U '%SYS'
    "##Class(Backup.General).IsWDSuspendedExt()"
    freeze_status=$?
    if [ $freeze_status -eq 5 ]; then
        echo "`date`: $INST is in frozen state"
        # Thaw
        # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
        $DOCKER_EXEC irissession $INST -U%SYS
        "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")"
        status=$?

        case $status in
            5) echo "`date`: $INST IS THAWED"
                $DOCKER_EXEC irissession $INST -U%SYS
                "##Class(Backup.General).ExternalSetHistory(\"$LOGFILE\")"
                ;;
            3) echo "`date`: $INST THAW FAILED"
                EXIT_CODE=202
                ;;
            *) echo "`date`: ERROR: Unknown status code: $status"
                EXIT_CODE=202
                ;;
        esac
        echo "`date`: Completed thaw of $INST"
    else
        echo "`date`: ERROR: $INST IS already THAWED"
        EXIT_CODE=205
    fi
done

```

```

        fi
    done
    echo "`date`: Post thaw script finished"
}

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        # return failure
        EXIT_CODE=1
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."
exit $EXIT_CODE

```

Pour plus d'informations, consultez le [GitHub référentiel](#).

Empty document template

```

###=====###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
this

```

```

# software and associated documentation files (the "Software"), to deal in the
# Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
  feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
    and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12})$
  command:
    # Data Lifecycle Manager will trigger the pre-script and post-script actions
    during policy execution.
    # 'dry-run' option is intended for validating the document execution without
    triggering any commands
    # on the instance. The following allowedValues will allow Data Lifecycle Manager
    to successfully
    # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
    be executed.
    allowedValues:
      - pre-script
      - post-script
      - dry-run

mainSteps:
- action: aws:runShellScript

```

```

description: Run Database freeze/thaw commands
name: run_pre_post_scripts
precondition:
  StringEquals:
    - platformType
    - Linux
inputs:
  runCommand:
    - |
      #!/bin/bash

```

```
###=====###
```

Error Codes

```
###=====###
```

```

# The following Error codes will inform Data Lifecycle Manager of the type of
error

```

```

# and help guide handling of the error.

```

```

# The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.

```

```

# 1 Pre-script failed during execution - 201

```

```

# 2 Post-script failed during execution - 202

```

```

# 3 Auto thaw occurred before post-script was initiated - 203

```

```

# 4 Pre-script initiated while post-script was expected - 204

```

```

# 5 Post-script initiated while pre-script was expected - 205

```

```

# 6 Application not ready for pre or post-script initiation - 206

```

```
###=====###
```

Global variables

```
###=====###
```

```

START=$(date +%s)

```

```

# For testing this script locally, replace the below with OPERATION=$1.

```

```

OPERATION={{ command }}

```

```

# Add all pre-script actions to be performed within the function below

```

```

execute_pre_script() {

```

```

    echo "INFO: Start execution of pre-script"

```

```

}

```

```

# Add all post-script actions to be performed within the function below

```

```

execute_post_script() {

```

```

    echo "INFO: Start execution of post-script"
}

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."

```

Une fois que vous avez obtenu le contenu de votre document SSM, utilisez l'une des procédures suivantes pour créer le document SSM personnalisé.

Console

Pour créer un document de commande SSM

1. Ouvrez la AWS Systems Manager console à l'adresse <https://console.aws.amazon.com/systems-manager/>.

2. Dans le volet de navigation, choisissez Documents, puis sélectionnez Créer un document, Commande ou session.
3. Pour Name (Nom), saisissez un nom évocateur pour le document.
4. Pour Type de cible, sélectionnez /AWS::EC2::Instance.
5. Pour Type de document, sélectionnez Commande.
6. Dans le champ Contenu, sélectionnez YAML, puis collez le contenu du document.
7. Dans la section Balises du document, ajoutez une balise avec une clé de balise `DLMScriptsAccess` et une valeur de balise `true`.

 Important

La `DLMScriptsAccess:true` balise est requise par la politique `AWSDataLifecycleManagerSSMFullAccess` AWS gérée utilisée à l'étape 3 : Préparation du rôle IAM d'Amazon Data Lifecycle Manager. La politique utilise la clé de condition `aws:ResourceTag` pour limiter l'accès aux documents SSM dotés de cette balise.

8. Sélectionnez Créer un document.

AWS CLI

Pour créer un document de commande SSM

Utilisez la commande [create-document](#). Pour `--name`, saisissez un nom descriptif pour le document. Pour `--document-type`, spécifiez `Command`. Pour `--content`, spécifiez le chemin d'accès au fichier `.yaml` avec le contenu du document SSM. Pour `--tags`, spécifiez `"Key=DLMScriptsAccess,Value=true"`.

```
$ aws ssm create-document \  
--content file://path/to/file/documentContent.yaml \  
--name "document_name" \  
--document-type "Command" \  
--document-format YAML \  
--tags "Key=DLMScriptsAccess,Value=true"
```

Étape 3 : Préparer le rôle IAM d'Amazon Data Lifecycle Manager

Note

Cette étape est nécessaire si :

- Vous créez ou mettez à jour une politique de capture pre/post d'écran activée par script qui utilise un rôle IAM personnalisé.
- Vous utilisez la ligne de commande pour créer ou mettre à jour une politique de capture instantanée pre/post activée par script qui utilise la politique par défaut.

Si vous utilisez la console pour créer ou mettre à jour une politique de capture d'écran pre/post activée par script qui utilise le rôle par défaut pour la gestion des captures instantanées (`AWSDataLifecycleManagerDefaultRole`), ignorez cette étape. Dans ce cas, la `AWSDataLifecycleManagerSSMFullAccess` politique est automatiquement associée à ce rôle.

Vous devez vous assurer que le rôle IAM que vous utilisez pour définir la politique accorde à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions SSM requises pour exécuter des pré-scripts et des post-scripts sur les instances ciblées par la politique.

Amazon Data Lifecycle Manager fournit une politique gérée (`AWSDataLifecycleManagerSSMFullAccess`) qui inclut les autorisations requises. Vous pouvez associer cette politique à votre rôle IAM de gestion des instantanés afin de vous assurer qu'elle inclut les autorisations.

Important

La politique `AWSDataLifecycleManagerSSMFullAccess` gérée utilise la clé de `aws:ResourceTag` condition pour restreindre l'accès à des documents SSM spécifiques lors de l'utilisation de pré-scripts et de post-scripts. Pour permettre à Amazon Data Lifecycle Manager d'accéder aux documents SSM, vous devez vous assurer que vos documents SSM sont balisés avec `DLMScriptsAccess:true`

Vous pouvez également créer manuellement une politique personnalisée ou attribuer les autorisations requises directement au rôle IAM que vous utilisez. Vous pouvez utiliser les mêmes

autorisations que celles définies dans la politique `AWSDatalifecycleManagerSSMFullAccess` gérée, mais la clé de `aws:ResourceTag` condition est facultative. Si vous décidez de ne pas inclure cette clé de condition, vous n'avez pas besoin de baliser vos documents SSM avec `DLMScriptsAccess:true`.

Utilisez l'une des méthodes suivantes pour ajouter la `AWSDatalifecycleManagerSSMFullAccess` politique à votre rôle IAM.

Console

Pour attacher la politique gérée à votre rôle personnalisé

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Recherchez et sélectionnez votre rôle personnalisé pour la gestion des instantanés.
4. Sous l'onglet Permissions (Autorisations), choisissez Add Permissions (Ajouter des autorisations), Attach policies (Attacher des politiques).
5. Recherchez et sélectionnez la politique `AWSDatalifecycleManagerSSMFullAccess` gérée, puis choisissez Ajouter des autorisations.

AWS CLI

Pour attacher la politique gérée à votre rôle personnalisé

Utilisez la commande [attach-role-policy](#). Pour `---role-name`, spécifiez le nom de votre rôle personnalisé. Pour `--policy-arn`, spécifiez `arn:aws:iam::aws:policy/AWSDatalifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDatalifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Étape 4 : Créer une politique de cycle de vie des instantanés

Pour automatiser les instantanés cohérents par rapport à l'application, vous devez créer une politique de cycle de vie des instantanés qui cible les instances, et configurer des pré-scripts et post-scripts pour cette politique.

Console

Pour créer la politique de cycle de vie des instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans la page Sélectionner un type de stratégie, choisissez Stratégie d'instantané EBS, puis Suivant.
4. Dans la section Ressources cibles, effectuez les opérations suivantes :
 - a. Pour Types de ressources cibles, choisissez Instance.
 - b. Pour Balises de ressource cible, spécifiez les balises de ressource qui identifient les instances à sauvegarder. Seules les ressources possédant les balises spécifiées seront sauvegardées.
5. Pour le rôle IAM, choisissez AWSDataLifecycleManagerDefaultRole (le rôle par défaut pour la gestion des instantanés) ou choisissez un rôle personnalisé que vous avez créé et préparé pour les pré-scripts et les post-scripts.
6. Configurez les planifications et les options supplémentaires selon les besoins. Nous vous recommandons de planifier les heures de création des instantanés pour des périodes correspondant à votre charge de travail, par exemple pendant les fenêtres de maintenance.

Pour SAP HANA, nous vous recommandons d'activer la restauration d'instantané rapide.

Note

Si vous activez une planification pour les sauvegardes VSS, vous ne pouvez pas activer Exclure des volumes de données spécifiques ou Copier les balises depuis la source.

7. Dans la section Pré-scripts et post-scripts, sélectionnez Activer les pré-scripts et post-scripts, puis effectuez les opérations suivantes, en fonction de votre charge de travail :
 - Pour créer des instantanés cohérents par rapport à l'application de vos applications Windows, sélectionnez Sauvegarde VSS.
 - Pour créer des instantanés cohérents par rapport à l'application de vos charges de travail SAP HANA, sélectionnez SAP HANA.

- Pour créer des instantanés cohérents avec les applications de toutes les autres bases de données et charges de travail, y compris vos bases de données MySQL, PostgreSQL ou InterSystems IRIS autogérées, à l'aide d'un document SSM personnalisé, sélectionnez Document SSM personnalisé.
 1. Pour Option d'automatisation, choisissez Pré-scripts et post-scripts.
 2. Pour Document SSM, sélectionnez le document SSM que vous avez préparé.
- 8. En fonction de l'option que vous avez sélectionnée, configurez les options supplémentaires suivantes :
 - Délai d'expiration du script : (document SSM personnalisé uniquement) délai d'expiration au terme duquel Amazon Data Lifecycle Manager échoue à exécuter le script si celui-ci n'est pas terminé. Si un script ne s'exécute pas dans le délai imparti, Amazon Data Lifecycle Manager échoue. Le délai d'expiration s'applique aux pré-scripts et post-scripts individuellement. Le délai d'expiration minimum et par défaut est de 10 secondes. Et le délai d'expiration maximum est de 120 secondes.
 - Relancer les scripts en échec : sélectionnez cette option pour relancer les scripts qui ne se terminent pas dans le délai imparti. En cas d'échec du pré-script, Amazon Data Lifecycle Manager relance l'intégralité du processus de création d'instantanés, y compris l'exécution des pré-scripts et post-scripts. Si le post-script échoue, Amazon Data Lifecycle Manager relance uniquement le post-script ; dans ce cas, le pré-script sera terminé et l'instantané aura peut-être été créé.
 - Prise par défaut d'instantanés en cas de panne : sélectionnez cette option pour utiliser par défaut des instantanés en cas de panne si le pré-script ne s'exécute pas. Il s'agit du comportement de création d'instantanés par défaut pour Amazon Data Lifecycle Manager si les pré-scripts et post-scripts ne sont pas activés. Si vous avez activé les relances, Amazon Data Lifecycle Manager utilise par défaut des instantanés en cas de panne uniquement une fois que toutes les relances ont été épuisées. Si le pré-script échoue et que vous n'utilisez pas par défaut des instantanés en cas de panne, Amazon Data Lifecycle Manager ne crée pas d'instantanés pour l'instance pendant cette exécution planifiée.

Note

Si vous créez des instantanés pour SAP HANA, vous souhaitez peut-être désactiver cette option. Crash-consistent les instantanés des charges de travail SAP HANA ne peuvent pas être restaurés de la même manière.

9. Choisissez Créer une politique par défaut.**Note**

Si vous obtenez l'erreur `Role with name AWSDatalifecycleManagerDefaultRole already exists`, consultez [Résoudre les problèmes liés à Amazon Data Lifecycle Manager](#) pour plus d'informations.

AWS CLI

Pour créer la politique de cycle de vie des instantanés

Utilisez la commande [create-lifecycle-policy](#) et incluez les paramètres `Scripts` dans `CreateRule`. Pour plus d'informations sur les paramètres, consultez la [référence d'API Amazon Data Lifecycle Manager](#).

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

Lorsque `policyDetails.json` inclut l'un des éléments suivants, selon votre cas d'utilisation :

- Sauvegarde VSS

```
{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
```

```

    "TargetTags": [{
      "Key": "tag_key",
      "Value": "tag_value"
    }],
    "Schedules": [{
      "Name": "schedule_name",
      "CreateRule": {
        "CronExpression": "cron_for_creation_frequency",
        "Scripts": [{
          "ExecutionHandler": "AWS_VSS_BACKUP",
          "ExecuteOperationOnScriptFailure": true/false,
          "MaximumRetryCount": retries (0-3)
        }]
      },
      "RetainRule": {
        "Count": retention_count
      }
    }]
  }
}

```

- Sauvegardes SAP HANA

```

{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "tag_key",
    "Value": "tag_value"
  }],
  "Schedules": [{
    "Name": "schedule_name",
    "CreateRule": {
      "CronExpression": "cron_for_creation_frequency",
      "Scripts": [{
        "Stages": ["PRE", "POST"],
        "ExecutionHandlerService": "AWS_SYSTEMS_MANAGER",
        "ExecutionHandler": "AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA",
        "ExecuteOperationOnScriptFailure": true/false,
        "ExecutionTimeout": timeout_in_seconds (10-120),
        "MaximumRetryCount": retries (0-3)
      }]
    }
  ]
}

```

```

    },
    "RetainRule": {
        "Count": retention_count
    }
  ]
}

```

- Document SSM personnalisé

```

{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "tag_key",
    "Value": "tag_value"
  }],
  "Schedules": [{
    "Name": "schedule_name",
    "CreateRule": {
      "CronExpression": "cron_for_creation_frequency",
      "Scripts": [{
        "Stages": ["PRE", "POST"],
        "ExecutionHandlerService": "AWS_SYSTEMS_MANAGER",
        "ExecutionHandler": "ssm_document_name|arn",
        "ExecuteOperationOnScriptFailure": true/false,
        "ExecutionTimeout": timeout_in_seconds (10-120),
        "MaximumRetryCount": retries (0-3)
      }]
    },
    "RetainRule": {
      "Count": retention_count
    }
  ]
}

```

Considérations relatives aux sauvegardes VSS avec Amazon Data Lifecycle Manager

Avec Amazon Data Lifecycle Manager, vous pouvez sauvegarder et restaurer les applications Windows compatibles avec VSS (Volume Shadow Copy Service) exécutées sur des instances Amazon EC2. Si l'application possède un enregistreur VSS enregistré auprès de Windows VSS,

Amazon Data Lifecycle Manager crée un instantané qui sera cohérent avec l'application pour cette application.

 Note

Amazon Data Lifecycle Manager ne prend actuellement en charge que les instantanés cohérents par rapport à l'application des ressources exécutées sur Amazon EC2, en particulier pour les scénarios de sauvegarde dans lesquels les données d'application peuvent être restaurées en remplaçant une instance existante par une nouvelle instance créée à partir de la sauvegarde. Les types d'instances ou applications ne sont pas tous pris en charge pour les sauvegardes VSS. Pour plus d'informations, consultez la section Instantanés [Application-consistent Windows VSS](#) dans le guide de l'utilisateur Amazon EC2.

Types d'instance non pris en charge

Les types d'instances Amazon EC2 suivants ne sont pas pris en charge pour les sauvegardes VSS. Si votre politique cible l'un de ces types d'instances, Amazon Data Lifecycle Manager peut toujours créer des sauvegardes VSS, mais les instantanés risquent de ne pas être balisés avec les balises système requises. Sans ces balises, les instantanés ne seront pas gérés par Amazon Data Lifecycle Manager après leur création. Vous aurez peut-être besoin de supprimer ces instantanés manuellement.

- T3 : t3.nano | t3.micro
- T3a : t3a.nano | t3a.micro
- T2 : t2.nano | t2.micro

Responsabilité partagée pour les instantanés cohérents par rapport à l'application

Vous devez vous assurer que :

- L'agent SSM est installé, à jour et s'exécute sur vos instances cibles
- Systems Manager est autorisé à effectuer les actions requises sur les instances cibles
- Amazon Data Lifecycle Manager est autorisé à effectuer les actions Systems Manager requises pour exécuter des pré-scripts et des post-scripts sur les instances cibles.

- Pour les charges de travail personnalisées, telles que les bases de données MySQL, PostgreSQL ou InterSystems IRIS autogérées, le document SSM que vous utilisez inclut les actions correctes et requises pour geler, vider et décongeler la configuration de votre base de données. I/O
- Les délais de création d'instantanés correspondent à votre planification de charge de travail. Par exemple, essayez de planifier la création d'instantanés pendant les fenêtres de maintenance planifiées.

Amazon Data Lifecycle Manager garantit que :

- la création d'instantanés démarre dans les 60 minutes suivant l'heure de création d'instantanés prévue ;
- les pré-scripts s'exécutent avant le lancement de la création d'instantanés ;
- les post-scripts s'exécutent une fois que le pré-script a réussi et que la création d'instantanés a été lancée ; Amazon Data Lifecycle Manager exécute le post-script uniquement si le pré-script aboutit ; si le pré-script échoue, Amazon Data Lifecycle Manager n'exécute pas le post-script ;
- les instantanés sont balisés avec les balises appropriées lors de leur création ;
- CloudWatch des métriques et des événements sont émis lorsque des scripts sont lancés et lorsqu'ils échouent ou réussissent.

Autres cas d'utilisation des pré-scripts et des post-scripts de Data Lifecycle Manager

Outre l'automatisation des instantanés cohérents par rapport à l'application, vous pouvez utiliser les pré-scripts et les post-scripts ensemble ou séparément pour automatiser d'autres tâches administratives avant ou après la création des instantanés. Par exemple :

- Utilisation d'un pré-script pour appliquer des correctifs avant la création d'instantanés. Cela peut vous aider à créer des instantanés après avoir appliqué vos mises à jour logicielles hebdomadaires ou mensuelles régulières.

Note

Si vous choisissez d'exécuter uniquement un pré-script, l'option Prise par défaut d'instantanés en cas de panne est activée par défaut.

- Utilisation d'un post-script pour appliquer des correctifs après la création d'instantanés. Cela peut vous aider à créer des instantanés avant d'appliquer vos mises à jour logicielles hebdomadaires ou mensuelles régulières.

Démarrage pour d'autres cas d'utilisation

Cette section explique les étapes à suivre lorsque vous utilisez des scripts de and/or pré-publication pour des cas d'utilisation autres que des instantanés cohérents avec les applications.

Étape 1 : Préparer les instances cibles

Pour préparer vos instances cibles pour les scripts de and/or pré-publication

1. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.
 - (instances Linux) Installation [manuelle de l'agent SSM sur des instances EC2 pour Linux](#)
 - (instances Windows) [Utilisation de l'agent SSM sur les instances EC2 pour Windows Server](#)
2. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez [Vérification du statut de l'SSM Agent et démarrage de l'agent](#).
3. Configurez Systems Manager pour des instances Amazon EC2. Pour plus d'informations, consultez [Configuration de Systems Manager pour des instances Amazon EC2](#) dans le Guide de l'utilisateur AWS Systems Manager .

Étape 2 : Préparer le document SSM

Vous devez créer un document de commande SSM qui inclut les scripts de and/or pré-publication avec les commandes que vous souhaitez exécuter.

Vous pouvez créer un document SSM à l'aide du modèle de document SSM vide ci-dessous et ajouter vos commandes pré-script et post-script dans les sections de document appropriées.

Notez ce qui suit :

- Il est de votre responsabilité de vous assurer que le document SSM exécute les actions correctes et requises pour votre charge de travail.
- Le document SSM doit inclure les champs obligatoires pour `allowedValues`, notamment `pre-script`, `post-script` et `dry-run`. Amazon Data Lifecycle Manager exécutera des

commandes sur votre instance en fonction du contenu de ces sections. Si votre document SSM ne contient pas ces sections, Amazon Data Lifecycle Manager le considérera comme un échec d'exécution.

```
###=====###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###=====###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
  feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre and/
or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12})$
  command:
    # Data Lifecycle Manager will trigger the pre-script and post-script actions during
policy execution.
    # 'dry-run' option is intended for validating the document execution without
triggering any commands
    # on the instance. The following allowedValues will allow Data Lifecycle Manager to
successfully
    # trigger pre and post script actions.
    type: String
    default: 'dry-run'
```

```

    description: (Required) Specifies whether pre-script and/or post-script should be
executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

###=====###
    ### Error Codes

###=====###
    # The following Error codes will inform Data Lifecycle Manager of the type of
error
    # and help guide handling of the error.
    # The Error code will also be emitted via AWS Eventbridge events in the 'cause'
field.
    # 1 Pre-script failed during execution - 201
    # 2 Post-script failed during execution - 202
    # 3 Auto thaw occurred before post-script was initiated - 203
    # 4 Pre-script initiated while post-script was expected - 204
    # 5 Post-script initiated while pre-script was expected - 205
    # 6 Application not ready for pre or post-script initiation - 206

###=====###
    ### Global variables

###=====###
    START=$(date +%s)
    # For testing this script locally, replace the below with OPERATION=$1.

```

```
OPERATION={{ command }}

# Add all pre-script actions to be performed within the function below
execute_pre_script() {
    echo "INFO: Start execution of pre-script"
}

# Add all post-script actions to be performed within the function below
execute_post_script() {
    echo "INFO: Start execution of post-script"
}

# Debug logging for parameters passed to the SSM document
echo "INFO: ${OPERATION} starting at $(date) with executionId: ${EXECUTION_ID}"

# Based on the command parameter value execute the function that supports
# pre-script/post-script operation
case ${OPERATION} in
    pre-script)
        execute_pre_script
        ;;
    post-script)
        execute_post_script
        ;;
    dry-run)
        echo "INFO: dry-run option invoked - taking no action"
        ;;
    *)
        echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
        exit 1 # return failure
        ;;
esac

END=$(date +%s)
# Debug Log for profiling the script time
echo "INFO: ${OPERATION} completed at $(date). Total runtime: $(( ${END} -
${START} )) seconds."
```

Étape 3 : Préparer le rôle IAM d'Amazon Data Lifecycle Manager

Note

Cette étape est nécessaire si :

- Vous créez ou mettez à jour une politique de capture pre/post d'écran activée par script qui utilise un rôle IAM personnalisé.
- Vous utilisez la ligne de commande pour créer ou mettre à jour une politique de capture instantanée pre/post activée par script qui utilise la politique par défaut.

Si vous utilisez la console pour créer ou mettre à jour une politique de capture d'écran pre/post activée par script qui utilise le rôle par défaut pour la gestion des captures instantanées (`AWSDataLifecycleManagerDefaultRole`), ignorez cette étape. Dans ce cas, la `AWSDataLifecycleManagerSSMFullAccess` politique est automatiquement associée à ce rôle.

Vous devez vous assurer que le rôle IAM que vous utilisez pour la politique accorde à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions SSM requises pour exécuter des pré-scripts et des post-scripts sur les instances ciblées par la politique.

Amazon Data Lifecycle Manager fournit une politique gérée (`AWSDataLifecycleManagerSSMFullAccess`) qui inclut les autorisations requises. Vous pouvez associer cette politique à votre rôle IAM de gestion des instantanés afin de vous assurer qu'elle inclut les autorisations.

Important

La politique `AWSDataLifecycleManagerSSMFullAccess` gérée utilise la clé de `aws:ResourceTag` condition pour restreindre l'accès à des documents SSM spécifiques lors de l'utilisation de pré-scripts et de post-scripts. Pour permettre à Amazon Data Lifecycle Manager d'accéder aux documents SSM, vous devez vous assurer que vos documents SSM sont balisés avec `DLMScriptsAccess:true`

Vous pouvez également créer manuellement une politique personnalisée ou attribuer les autorisations requises directement au rôle IAM que vous utilisez. Vous pouvez utiliser les mêmes

autorisations que celles définies dans la politique `AWSDataLifecycleManagerSSMFullAccess` gérée, mais la clé de `aws:ResourceTag` condition est facultative. Si vous décidez de ne pas utiliser cette clé de condition, vous n'avez pas besoin de baliser vos documents SSM avec `DLMScriptsAccess:true`.

Utilisez l'une des méthodes suivantes pour ajouter la `AWSDataLifecycleManagerSSMFullAccess` politique à votre rôle IAM.

Console

Pour attacher la politique gérée à votre rôle personnalisé

1. Ouvrez la console IAM à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Recherchez et sélectionnez votre rôle personnalisé pour la gestion des instantanés.
4. Sous l'onglet Permissions (Autorisations), choisissez Add Permissions (Ajouter des autorisations), Attach policies (Attacher des politiques).
5. Recherchez et sélectionnez la politique `AWSDataLifecycleManagerSSMFullAccess` gérée, puis choisissez Ajouter des autorisations.

AWS CLI

Pour attacher la politique gérée à votre rôle personnalisé

Utilisez la commande [attach-role-policy](#). Pour `---role-name`, spécifiez le nom de votre rôle personnalisé. Pour `--policy-arn`, spécifiez `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Création d'une politique de cycle de vie des instantanés

Console

Pour créer la politique de cycle de vie des instantanés

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans la page Sélectionner un type de stratégie, choisissez Stratégie d'instantané EBS, puis Suivant.
4. Dans la section Ressources cibles, effectuez les opérations suivantes :
 - a. Pour Types de ressources cibles, choisissez Instance.
 - b. Pour Balises de ressource cible, spécifiez les balises de ressource qui identifient les instances à sauvegarder. Seules les ressources possédant les balises spécifiées seront sauvegardées.
5. Pour le rôle IAM, choisissez AWSDataLifecycleManagerDefaultRole (le rôle par défaut pour la gestion des instantanés) ou choisissez un rôle personnalisé que vous avez créé et préparé pour les pré-scripts et les post-scripts.
6. Configurez les planifications et les options supplémentaires selon les besoins. Nous vous recommandons de planifier les heures de création des instantanés pour des périodes correspondant à votre charge de travail, par exemple pendant les fenêtres de maintenance.
7. Dans la section Pré-scripts et post-scripts, sélectionnez Activer les pré-scripts et post-scripts, puis effectuez les opérations suivantes :
 - a. Sélectionnez Document SSM personnalisé.
 - b. Pour Option d'automatisation, choisissez l'option qui correspond aux scripts que vous souhaitez exécuter.
 - c. Pour Document SSM, sélectionnez le document SSM que vous avez préparé.
8. Configurez les options supplémentaires suivantes au besoin :
 - Délai d'expiration du script : délai d'expiration au terme duquel Amazon Data Lifecycle Manager échoue à exécuter le script si celui-ci n'est pas terminé. Si un script ne s'exécute pas dans le délai imparti, Amazon Data Lifecycle Manager échoue. Le délai d'expiration

s'applique aux pré-scripts et post-scripts individuellement. Le délai d'expiration minimum et par défaut est de 10 secondes. Et le délai d'expiration maximum est de 120 secondes.

- Relancer les scripts en échec : sélectionnez cette option pour relancer les scripts qui ne se terminent pas dans le délai imparti. En cas d'échec du pré-script, Amazon Data Lifecycle Manager relance l'intégralité du processus de création d'instantanés, y compris l'exécution des pré-scripts et post-scripts. Si le post-script échoue, Amazon Data Lifecycle Manager relance uniquement le post-script ; dans ce cas, le pré-script sera terminé et l'instantané aura peut-être été créé.
- Prise par défaut d'instantanés en cas de panne : sélectionnez cette option pour utiliser par défaut des instantanés en cas de panne si le pré-script ne s'exécute pas. Il s'agit du comportement de création d'instantanés par défaut pour Amazon Data Lifecycle Manager si les pré-scripts et post-scripts ne sont pas activés. Si vous avez activé les relances, Amazon Data Lifecycle Manager utilise par défaut des instantanés en cas de panne uniquement une fois que toutes les relances ont été épuisées. Si le pré-script échoue et que vous n'utilisez pas par défaut des instantanés en cas de panne, Amazon Data Lifecycle Manager ne crée pas d'instantanés pour l'instance pendant cette exécution planifiée.

9. Choisissez Créer une politique par défaut.

Note

Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consultez [Résoudre les problèmes liés à Amazon Data Lifecycle Manager](#) pour plus d'informations.

AWS CLI

Pour créer la politique de cycle de vie des instantanés

Utilisez la commande [create-lifecycle-policy](#) et incluez les paramètres `Scripts` dans `CreateRule`. Pour plus d'informations sur les paramètres, consultez la [référence d'API Amazon Data Lifecycle Manager](#).

```
$ aws dlm create-lifecycle-policy \  
--description "policy_description" \  
--state ENABLED \  

```



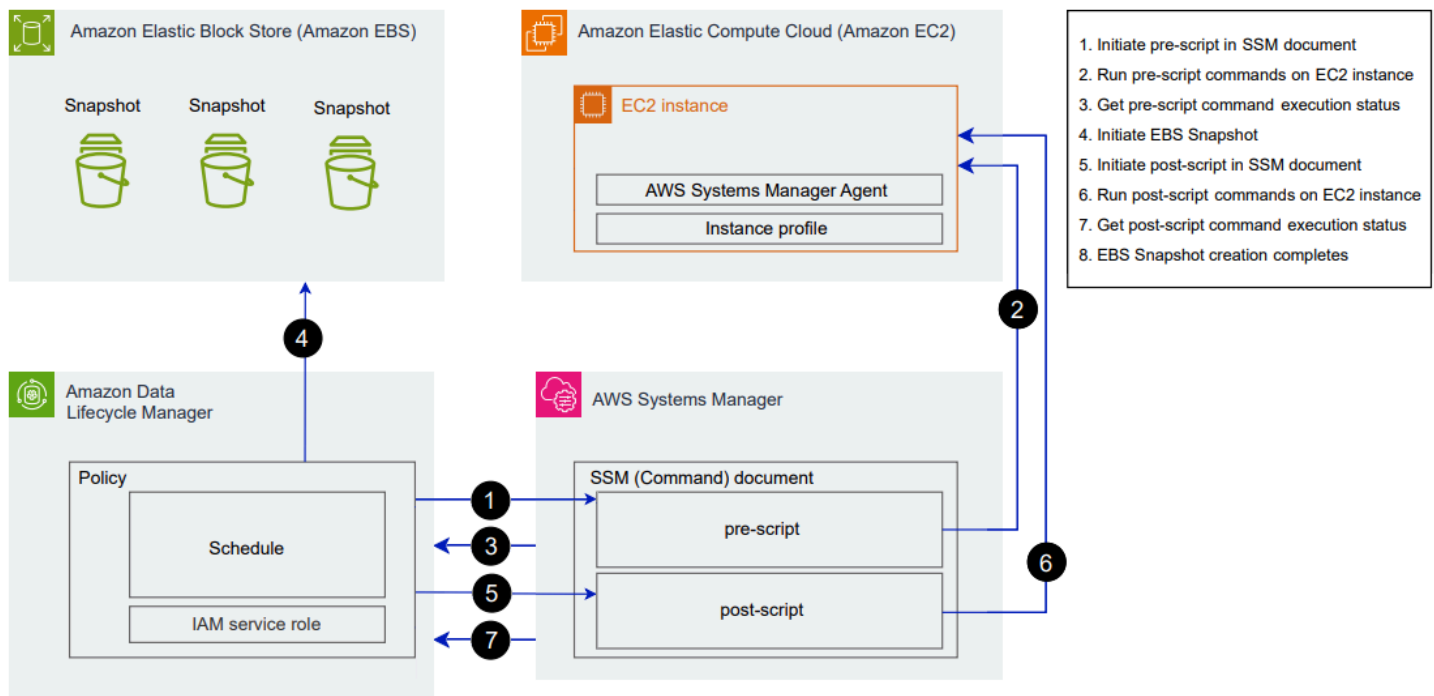
```
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

Où `policyDetails.json` inclut les éléments suivants.

```
{
  "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "tag_key",
    "Value": "tag_value"
  }],
  "Schedules": [{
    "Name": "schedule_name",
    "CreateRule": {
      "CronExpression": "cron_for_creation_frequency",
      "Scripts": [{
        "Stages": ["PRE" | "POST" | "PRE", "POST"],
        "ExecutionHandlerService": "AWS_SYSTEMS_MANAGER",
        "ExecutionHandler": "ssm_document_name|arn",
        "ExecuteOperationOnScriptFailure": true/false,
        "ExecutionTimeout": timeout_in_seconds (10-120),
        "MaximumRetryCount": retries (0-3)
      }]
    },
    "RetainRule": {
      "Count": retention_count
    }
  }]
}
```

Comment fonctionnent les pré-scripts et les post-scripts d'Amazon Data Lifecycle Manager

L'image suivante montre le flux de processus pour les pré-scripts et les post-scripts lors de l'utilisation de documents SSM personnalisés. Cela ne s'applique pas aux sauvegardes VSS.



Au moment prévu de la création d'instantanés, les actions et interactions entre services suivantes se produisent.

1. Amazon Data Lifecycle Manager lance l'action de pré-script en appelant le document SSM et en transmettant le paramètre `pre-script`.

Note

Les étapes 1 à 3 se produisent uniquement si vous exécutez des pré-scripts. Si vous exécutez uniquement des post-scripts, les étapes 1 à 3 sont ignorées.

2. Systems Manager envoie des commandes de pré-script à l'agent SSM exécuté sur les instances cibles. L'agent SSM exécute les commandes sur l'instance et renvoie les informations sur les statuts à Systems Manager.

Par exemple, si le document SSM est utilisé pour créer des instantanés cohérents avec les applications, le pré-script peut se figer et se vider I/O pour s'assurer que toutes les données mises en mémoire tampon sont écrites sur le volume avant la prise de l'instantané.

3. Systems Manager envoie des mises à jour du statut des commandes pré-script à Amazon Data Lifecycle Manager. Si le pré-script échoue, Amazon Data Lifecycle Manager effectue l'une des actions suivantes, en fonction de votre configuration des options de pré-script et de post-script :

Relances	Instantanés en cas de panne par défaut	Action
Activées avec des relances restantes	Activées	Relance du script jusqu'à ce qu'il réussisse ou que les relances soient épuisées
Épuisées sans exécution réussie	Activé	Création d'instantanés en cas de panne, sans exécution de post-script.
Activées avec des relances restantes	Désactivées	Relance du script jusqu'à ce qu'il réussisse ou que les relances soient épuisées
Épuisées sans exécution réussie	Désactivé	Création d'instantanés ignorée pour l'instance cible, sans exécution de post-script.
Désactivé	Activé	Création d'instantanés en cas de panne, sans exécution de post-script.
Désactivé	Désactivé	Création d'instantanés ignorée pour l'instance cible, sans exécution de post-script.

- Amazon Data Lifecycle Manager lance la création d'instantanés.
- Amazon Data Lifecycle Manager lance l'action de post-script en appelant le document SSM et en transmettant le paramètre `post-script`.

 Note

Les étapes 5 à 7 se produisent uniquement si vous exécutez des pré-scripts. Si vous exécutez uniquement des post-scripts, les étapes 1 à 3 sont ignorées.

6. Systems Manager envoie des commandes de post-script à l'agent SSM exécuté sur les instances cibles. L'agent SSM exécute les commandes sur l'instance et renvoie les informations sur les statuts à Systems Manager.

Par exemple, si le document SSM permet des instantanés cohérents avec les applications, ce post-script peut être dégelé I/O pour garantir que vos bases de données reprennent leurs I/O opérations normales après la prise de l'instantané.

7. Si vous exécutez un post-script et que Systems Manager indique qu'il s'est correctement terminé, le processus se termine.

Si le post-script échoue, Amazon Data Lifecycle Manager effectue l'une des actions suivantes, en fonction de votre configuration des options de pré-script et de post-script :

Nouvelles tentatives	Action
Activées avec des relances restantes	Relance du post-script jusqu'à ce qu'il réussisse ou que les relances soient épuisées
Épuisées sans succès	Post-script ignoré
Désactivé	Post-script ignoré

N'oubliez pas qu'en cas d'échec du post-script, le pré-script (s'il est activé) se termine avec succès et les instantanés ont peut-être été créés. Vous devrez peut-être prendre des mesures supplémentaires sur l'instance pour vous assurer qu'elle fonctionne comme prévu. Par exemple, si le pré-script a été suspendu et vidé I/O, mais que le post-script n'a pas réussi à dégeler I/O, vous devrez peut-être configurer votre base de données pour qu'elle soit dégelée automatiquement I/O ou vous devrez la décongeler manuellement. I/O

8. Le processus de création d'instantanés peut se terminer une fois le post-script terminé. Le temps nécessaire pour terminer l'instantané dépend de la taille de l'instantané.

Identifiez les instantanés créés avec les pré-scripts et les post-scripts de Data Lifecycle Manager

Amazon Data Lifecycle Manager attribue automatiquement les balises système suivantes aux instantanés créés à l'aide de pré-scripts et de post-scripts.

- Clé : `aws:dlm:pre-script` ; Valeur : `SUCCESS|FAILED`

Une valeur de balise de `SUCCESS` indique que le pré-script a été exécuté correctement. Une valeur de balise de `FAILED` indique que le pré-script n'a pas été exécuté correctement.

- Clé : `aws:dlm:post-script` ; Valeur : `SUCCESS|FAILED`

Une valeur de balise de `SUCCESS` indique que le post-script a été exécuté correctement. Une valeur de balise de `FAILED` indique que le post-script n'a pas été exécuté correctement.

Pour les documents SSM personnalisés et les sauvegardes SAP HANA, vous pouvez déduire la création réussie d'un instantané cohérent par rapport à l'application si l'instantané est balisé avec `aws:dlm:pre-script:SUCCESS` et `aws:dlm:post-script:SUCCESS`.

En outre, les instantanés cohérents par rapport à l'application créés à l'aide de la sauvegarde VSS sont automatiquement balisés avec :

- Clé : `AppConsistent tag` ; Valeur : `true|false`

Une valeur de balise égale à `true` indique que la sauvegarde VSS a réussi et que les instantanés sont cohérents avec l'application. Une valeur de balise égale à `false` indique que la sauvegarde VSS n'a pas réussi et que les instantanés ne sont pas cohérents avec l'application.

Surveillez les pré-scripts et les post-scripts d'Amazon Data Lifecycle Manager

Statistiques CloudWatch Amazon

Amazon Data Lifecycle Manager publie les CloudWatch mesures suivantes en cas d'échec et de réussite des pré-scripts et en cas d'échec et de réussite des sauvegardes VSS.

- `PreScriptStarted`
- `PreScriptCompleted`
- `PreScriptFailed`
- `PostScriptStarted`
- `PostScriptCompleted`
- `PostScriptFailed`
- `VSSBackupStarted`

- VSSBackupCompleted
- VSSBackupFailed

Pour de plus amples informations, veuillez consulter [Surveillez les politiques du Data Lifecycle Manager à l'aide de CloudWatch](#).

Amazon EventBridge

Amazon Data Lifecycle Manager émet l' EventBridge événement Amazon suivant lorsqu'un pré-script ou un post-script est lancé, réussit ou échoue

- DLM Pre Post Script Notification

Pour de plus amples informations, veuillez consulter [Surveillez les politiques du Data Lifecycle Manager à l'aide de EventBridge](#).

Création d'une politique personnalisée Amazon Data Lifecycle Manager pour les EBS-backed AMI

La procédure suivante explique comment utiliser Amazon Data Lifecycle Manager pour automatiser les cycles de vie des EBS-backed AMI.

Rubriques

- [Pour créer une politique de cycle de vie d'AMI](#)
- [Considérations relatives aux stratégies de cycle de vie des AMI](#)
- [Ressources supplémentaires](#)

Pour créer une politique de cycle de vie d'AMI

Utilisez l'une des procédures suivantes pour créer une politique de cycle de vie d'AMI.

Console

Pour créer une politique d'AMI

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Sur l'écran Sélectionner le type de politique, choisissez la stratégie EBS-backed AMI, puis cliquez sur Suivant.
4. Dans la section Ressources cibles, pour Etiquettes de ressources cibles, choisissez les étiquettes de ressources qui identifient les volumes ou les instances à sauvegarder. La politique sauvegarde uniquement les ressources ayant la clé de balise et les paires de valeurs spécifiées.
5. Pour Description, saisissez une brève description pour la stratégie.
6. Pour Rôle IAM, choisissez le rôle IAM autorisé à gérer des AMI et des instantanés, ainsi qu'à décrire des instances. Pour utiliser le rôle par défaut fourni par Amazon Data Lifecycle Manager, choisissez Rôle par défaut. Autrement, pour utiliser un rôle IAM personnalisé que vous avez créé précédemment, sélectionnez Choisir un autre rôle, puis sélectionnez le rôle à utiliser.
7. Pour Etiquettes de stratégie, ajoutez les étiquettes à appliquer à la stratégie de cycle de vie. Vous pouvez utiliser ces étiquettes pour identifier et catégoriser vos politiques.
8. Pour Statut de la stratégie après création, choisissez Activer la stratégie pour lancer l'exécutions de la stratégie lors de la prochaine heure planifiée ou Désactiver la stratégie pour empêcher l'exécution de la stratégie. Si vous n'activez pas la politique maintenant, elle ne commencera à créer des AMI que quand vous l'aurez activée manuellement après sa création.
9. Dans la section Redémarrage d'instance, indiquez si les instances doivent être redémarrées avant la création de l'AMI. Pour empêcher le redémarrage des instances ciblées, choisissez Non. Le choix de Non peut occasionner des problèmes de cohérence des données. Pour redémarrer les instances avant la création de l'AMI, choisissez Oui. Ce choix garantit la cohérence des données, mais peut entraîner le redémarrage simultané de plusieurs instances ciblées.
10. Choisissez Suivant.
11. Dans l'écran Configurer une planification, configurez les planifications de stratégie. Une politique peut avoir jusqu'à quatre planifications. La planification 1 est obligatoire. Les planifications 2, 3 et 4 sont facultatives. Pour chaque planification de politique que vous ajoutez, procédez comme suit :
 - a. Dans la section Détails de la planification, procédez comme suit :

- i. Pour Nom de la planification, spécifiez un nom descriptif pour la planification.
- ii. Pour Fréquence et les champs associés, configurez l'intervalle entre les exécutions de stratégie.

Vous pouvez configurer les exécutions de politique selon une planification quotidienne, hebdomadaire, mensuelle ou annuelle. Vous pouvez également sélectionner Expression cron personnalisée pour spécifier un intervalle allant jusqu'à un an. Pour plus d'informations, consultez la section Expressions [cron et rate](#) dans le guide de l' EventBridge utilisateur Amazon.

- iii. Pour Démarrage à, spécifiez l'heure de démarrage des exécutions de la stratégie. La première exécution de la politique commence dans l'heure qui suit l'heure que vous planifiez. L'heure doit être au format UTC hh:mm.
- iv. Pour Type de rétention, spécifiez la stratégie de rétention des AMI créées par la planification.

Vous pouvez retenir les AMI en fonction de leur nombre total ou de leur âge.

Pour la rétention basée sur le nombre, la plage s'étend de 1 à 1000. Une fois le nombre maximum atteint, l'AMI la plus ancienne est supprimée lors de la création d'une nouvelle AMI.

Pour la rétention basée sur l'âge, la plage s'étend de 1 jour à 100 ans. Une fois la période de rétention de chaque AMI expirée, celle-ci est supprimée.

 Note

Toutes les planifications doivent avoir le même type de conservation. Vous pouvez spécifier le type de conservation pour la planification 1 uniquement. Les planifications 2, 3 et 4 héritent du type de conservation de la planification 1. Chaque planification peut avoir son propre nombre ou sa propre période de conservation.

- b. Configurez le balisage pour les AMI.

Dans la section Etiquetage, procédez comme suit :

- i. Pour copier toutes les étiquettes définies par l'utilisateur à partir de l'instance source vers les AMI créées par la planification, sélectionnez Copier les étiquettes à partir de la source.
 - ii. Par défaut, les AMI créées par la planification sont automatiquement étiquetées avec l'ID de l'instance source. Afin d'empêcher ce balisage automatique, pour Etiquettes de variables, supprimez la vignette `instance-id:${instance-id}`.
 - iii. Pour spécifier des étiquettes supplémentaires à attribuer aux AMI créées par cette planification, choisissez Ajouter des étiquettes.
- c. Configurez l'obsolescence des AMI.

Pour rendre obsolètes les AMI lorsqu'elles ne doivent plus être utilisées, dans le champ AMI deprecation (Obsolescence d'AMI), sélectionnez Enable AMI deprecation for this schedule (Activer l'obsolescence des AMI pour cette planification), puis spécifiez la règle d'obsolescence des AMI. La règle d'obsolescence des AMI spécifie quand les AMI deviennent obsolètes.

Si la planification utilise la rétention d'AMI basée sur le nombre, vous devez spécifier le nombre d'AMI les plus anciennes à rendre obsolètes. Le nombre d'obsolescences doit être inférieur ou égal au nombre de rétention d'AMI de la planification, et il ne peut être supérieur à 1 000. Par exemple, si la planification est configurée pour conserver un maximum de 5 AMI, vous pouvez configurer la planification pour rendre obsolètes jusqu'à 5 anciennes AMI.

Si la planification utilise la rétention d'AMI basée sur l'âge, vous devez spécifier la période après laquelle les AMI deviennent obsolètes. Le délai d'obsolescence doit être inférieur ou égal à la période de rétention d'AMI du planificateur, et il ne peut pas être supérieur à 10 ans (soit 120 mois, 520 semaines ou 3 650 jours). Par exemple, si la planification est configurée pour conserver les AMI pendant 10 jours, vous pouvez configurer les AMI planifiées pour les rendre obsolètes après des périodes allant jusqu'à 10 jours après leur création.

- d. Configurez la copie entre régions.

Pour copier les AMI créées par le calendrier vers différentes régions, dans la section Cross-Region Copie, sélectionnez Activer la copie entre régions. Vous pouvez copier des AMI vers jusqu'à trois régions supplémentaires dans votre compte. Vous devez spécifier une règle de copie entre régions distincte pour chaque région de destination.

Pour chaque Région de destination, vous pouvez spécifier les informations suivantes :

- Règle de rétention pour les copies d'AMI. Lorsque la période de rétention expire, la copie dans la Région de destination est automatiquement supprimée.
- Statut de chiffrement des copies d'AMI. Si l'AMI source est chiffrée, ou si le chiffrement par défaut est activé, alors les AMI copiées sont chiffrées. Si l'AMI source n'est pas chiffrée et que le chiffrement par défaut est désactivé, vous pouvez activer le chiffrement. Si vous ne spécifiez pas de clé KMS, les AMI sont chiffrées à l'aide de la clé KMS par défaut pour le chiffrement EBS dans chaque région de destination. Si vous spécifiez une clé KMS pour la Région de destination, le rôle IAM sélectionné doit avoir accès à la clé KMS.
- Règle d'obsolescence pour les copies d'AMI. Les copies d'AMI deviennent automatiquement obsolètes lorsque la période d'obsolescence expire. La période d'obsolescence doit être inférieure ou égale à la période de rétention de la copie et ne peut être supérieure à 10 ans.
- Que ce soit pour copier toutes les balises ou aucune balise de l'AMI source.

 Note

Ne dépassez pas le nombre de copies d'AMI simultanées par région.

- e. Pour ajouter des planifications, choisissez l'option Ajouter une planification en haut de l'écran. Pour chaque planification supplémentaire, remplissez les champs comme décrit précédemment dans cette rubrique.
 - f. Après avoir ajouté les planifications requises, choisissez Examiner une stratégie.
12. Examinez le récapitulatif de la stratégie, puis choisissez Créer une stratégie.

 Note

Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, consultez [Résoudre les problèmes liés à Amazon Data Lifecycle Manager](#) pour plus d'informations.

Command line

Utilisez la commande [create-lifecycle-policy](#) pour créer une stratégie de cycle de vie d'AMI. Pour `PolicyType`, spécifiez `IMAGE_MANAGEMENT`.

Note

Pour simplifier la syntaxe, les exemples suivants utilisent un fichier JSON, `policyDetails.json`, qui comportent les détails de la stratégie.

Exemple 1 : Age-based rétention et dépréciation de l'AMI

Cet exemple présente une stratégie de cycle de vie d'AMI qui crée des AMI de toutes les instances qui possèdent une clé de balise `purpose` avec une valeur de `production` sans redémarrer les instances ciblées. La politique comporte une planification qui crée une AMI tous les jours à 01:00 (UTC). La politique conserve les AMI pour 2 jours et les rend obsolètes après 1 jour. Elle copie également les étiquettes de l'instance source vers les AMI qu'elle crée.

```
aws dlm create-lifecycle-policy \
  --description "My AMI policy" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
  --policy-details file:///policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
  "PolicyType": "IMAGE_MANAGEMENT",
  "ResourceTypes": [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "purpose",
    "Value": "production"
  }],
  "Schedules": [{
    "Name": "DailyAMIs",
    "TagsToAdd": [{
```

```

        "Key": "type",
        "Value": "myDailyAMI"
    }],
    "CreateRule": {
        "Interval": 24,
        "IntervalUnit": "HOURS",
        "Times": [
            "01:00"
        ]
    },
    "RetainRule": {
        "Interval": 2,
        "IntervalUnit": "DAYS"
    },
    "DeprecateRule": {
        "Interval": 1,
        "IntervalUnit": "DAYS"
    },
    "CopyTags": true
}
],
"Parameters": {
    "NoReboot": true
}
}

```

Si la demande aboutit, la commande renvoie l’ID de la politique nouvellement créée. Voici un exemple de sortie.

```

{
  "PolicyId": "policy-9876543210abcdef0"
}

```

Exemple 2 : Count-based conservation et dépréciation de l'AMI avec copie interrégionale

Cet exemple présente une politique de cycle de vie d’AMI qui crée des AMI de toutes les instances qui possèdent une clé de balise de `purpose` avec une valeur de `production` et redémarre les instances ciblées. La politique comporte une planification qui crée une AMI toutes les 6 heures à partir de 17:30 (UTC). La politique conserve les AMI 3 et rend automatiquement obsolètes les AMI 2 les plus anciennes. Elle comprend également une règle de copie inter-Régions qui copie les AMI dans `us-east-1`, conserve copies d’AMI 2 et rend automatiquement obsolète l’AMI la plus ancienne.

```
aws dlm create-lifecycle-policy \
  --description "My AMI policy" \
  --state ENABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
  --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
  "PolicyType": "IMAGE_MANAGEMENT",
  "ResourceTypes" : [
    "INSTANCE"
  ],
  "TargetTags": [{
    "Key": "purpose",
    "Value": "production"
  }],
  "Parameters" : {
    "NoReboot": true
  },
  "Schedules" : [{
    "Name" : "Schedule1",
    "CopyTags": true,
    "CreateRule" : {
      "Interval": 6,
      "IntervalUnit": "HOURS",
      "Times" : ["17:30"]
    },
    "RetainRule":{
      "Count" : 3
    },
    "DeprecateRule":{
      "Count" : 2
    },
    "CrossRegionCopyRules": [{
      "TargetRegion": "us-east-1",
      "Encrypted": true,
      "RetainRule":{
        "IntervalUnit": "DAYS",
        "Interval": 2
      },
      "DeprecateRule":{
```

```
        "IntervalUnit": "DAYS",
        "Interval": 1
    },
    "CopyTags": true
  ]
}
```

Considérations relatives aux stratégies de cycle de vie des AMI

Les considérations générales suivantes s'appliquent lors de la création de stratégies de cycle de vie d'AMI :

- Les politiques de cycle de vie des AMI ciblent uniquement les instances qui se trouvent dans la même région que la politique.
- La première opération de création d'AMI démarre dans l'heure suivant l'heure de début spécifiée. Les opérations suivantes de création d'AMI démarrent dans l'heure suivant leur heure planifiée.
- Lorsque Amazon Data Lifecycle Manager désenregistre une AMI, il la supprime automatiquement.
- Les balises de ressource cible sont sensibles à la casse.
- Si vous supprimez les balises cibles d'une instance ciblée par une politique, Amazon Data Lifecycle Manager ne gère plus les AMI existantes dans la norme. Vous devez les supprimer manuellement si elles ne sont plus nécessaires.
- Vous pouvez créer plusieurs stratégies pour sauvegarder une instance . Par exemple, si une instance comporte deux identifications, l'identification A étant la cible de la politique A qui permet de créer une AMI toutes les 12 heures et l'identification B étant la cible de la politique B qui permet de créer une AMI toutes les 24 heures, Amazon Data Lifecycle Manager crée des AMI en fonction des planifications des deux politiques. Vous pouvez également obtenir le même résultat en créant une seule politique comportant plusieurs planifications. Par exemple, vous pouvez créer une politique unique qui cible uniquement la balise A et spécifier deux planifications : l'une pour toutes les 12 heures et l'autre pour toutes les 24 heures.
- Les nouveaux volumes attachés à une instance cible après la création de la stratégie sont automatiquement inclus dans la sauvegarde lors de la prochaine exécution de la stratégie. Tous les volumes attachés à l'instance au moment de l'exécution de la politique sont inclus.
- Si vous créez une stratégie avec une planification personnalisée basée sur les crons configurée pour créer une seule AMI, la stratégie ne désenregistrera pas automatiquement cette AMI lorsque

le seuil de rétention est atteint. Vous devez désenregistrer manuellement l'AMI si elle n'est plus nécessaire.

- Si vous créez une politique basée sur l'âge dans laquelle la période de conservation est plus courte que la fréquence de création, Amazon Data Lifecycle Manager conservera toujours la dernière AMI jusqu'à la création de la suivante. Par exemple, si une politique basée sur l'âge crée une AMI par mois avec une période de conservation de sept jours, Amazon Data Lifecycle Manager conservera chaque AMI pendant un mois, même si la période de conservation est de sept jours.
- Pour les politiques basées sur le nombre, Amazon Data Lifecycle Manager crée toujours des AMI en fonction de la fréquence de création avant de tenter de désenregistrer l'AMI la plus ancienne, conformément à la politique de rétention.
- Le désenregistrement d'une AMI et la suppression des instantanés de sauvegarde associés peuvent prendre plusieurs heures. Si Amazon Data Lifecycle Manager crée l'AMI suivante avant que l'AMI précédemment créée ne soit correctement désenregistrée, vous pouvez conserver temporairement un nombre d'AMI supérieur à votre nombre de conservation.

Les considérations suivantes s'appliquent à la résiliation des instances ciblées par une politique :

- Si vous résiliez une instance qui était ciblée par une politique avec une planification de la rétention basée sur le nombre, la politique ne gère plus les AMI qu'elle a précédemment créés à partir de l'instance résiliée. Vous devez désenregistrer manuellement ces AMI précédents lorsqu'ils ne sont plus nécessaires.
- Si vous résiliez une instance qui était ciblée par une politique avec une planification de rétention basée sur l'âge, la politique continue à désenregistrer les AMI qui ont été précédemment créés à partir de l'instance résiliée selon la planification définie, jusqu'au dernier AMI, mais sans l'inclure. Vous devez désenregistrer manuellement la dernière AMI si elle n'est plus nécessaire.

Les considérations suivantes s'appliquent aux politiques d'AMI et à l'obsolescence des AMI :

- Si vous augmentez le nombre d'AMI à rendre obsolètes pour une planification avec rétention basée sur le nombre, la modification sera appliquée à toutes les AMI (existantes et nouvelles) créées par la planification.
- Si vous augmentez la période d'obsolescence de l'AMI pour une planification avec rétention basée sur l'âge, la modification sera uniquement appliquée aux nouvelles AMI. Les AMI existantes ne sont pas affectées.

- Si vous supprimez la règle d'obsolescence d'AMI d'une planification, Amazon Data Lifecycle Manager n'annulera pas l'obsolescence pour les AMI qui étaient précédemment obsolètes conformément à cette planification.
- Si vous supprimez la règle d'obsolescence d'AMI d'une planification, Amazon Data Lifecycle Manager n'annulera pas l'obsolescence pour les AMI qui étaient précédemment obsolètes conformément à cette planification.
- Si vous rendez manuellement obsolète une AMI créée par une politique d'AMI, Amazon Data Lifecycle Manager ne remplacera pas l'obsolescence.
- Si vous annulez manuellement l'obsolescence d'une AMI précédemment rendue obsolète par une politique AMI, Amazon Data Lifecycle Manager ne remplacera pas l'annulation.
- Si une AMI est créée par plusieurs planifications conflictuelles et qu'une ou plusieurs de ces planifications n'ont pas de règle d'obsolescence des AMI, Amazon Data Lifecycle Manager ne rendra pas cette AMI obsolète.
- Si une AMI est créée par plusieurs planifications conflictuelles et que toutes ces planifications disposent d'une règle d'obsolescence des AMI, Amazon Data Lifecycle Manager utilisera la règle d'obsolescence qui donne la date d'obsolescence la plus tardive.

Les considérations suivantes s'appliquent aux politiques AMI et à la [corbeille](#) :

- Si Amazon Data Lifecycle Manager annule l'enregistrement d'une AMI et l'envoie à la corbeille lorsque le seuil de rétention de la politique est atteint, et que vous restaurez manuellement l'AMI à partir de la corbeille, vous devez annuler manuellement l'enregistrement de cette AMI lorsqu'elle n'est plus nécessaire. Amazon Data Lifecycle Manager ne gèrera plus l'AMI.
- Si vous annulez manuellement l'enregistrement d'une AMI créée par une politique et que cette AMI se trouve dans la corbeille lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager n'annule pas l'enregistrement de l'AMI. Amazon Data Lifecycle Manager ne gère pas les AMI lorsqu'elles sont dans la corbeille.

Si l'AMI est restaurée à partir de la corbeille avant que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager annule l'enregistrement de l'AMI lorsque le seuil de rétention de la politique est atteint.

Si l'AMI est restaurée à partir de la corbeille après que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager n'annule plus l'enregistrement de l'AMI. Vous devez la supprimer manuellement lorsqu'elle n'est plus nécessaire.

Les considérations suivantes s'appliquent aux politiques d'AMI qui sont à l'état d'erreur :

- Pour les politiques avec des planifications de rétention basées sur l'âge, les AMI qui sont configurés pour expirer alors que la politique est dans l'état `error` sont conservés indéfiniment. Vous devez annuler l'enregistrement des AMI manuellement. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend l'annulation de l'enregistrement des AMI à mesure que leurs périodes de rétention expirent.
- Pour les politiques avec des planifications de rétention basée sur le nombre, la politique arrête de créer et d'annuler l'enregistrement des AMI pendant qu'elle est dans l'état `error`. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la création des AMI, ainsi que l'annulation de l'enregistrement des AMI lorsque le seuil de rétention est atteint.

Les considérations suivantes s'appliquent aux politiques relatives aux AMI et à la [désactivation des AMI](#) :

- Si vous désactivez une AMI créée par Amazon Data Lifecycle Manager et que cette AMI est désactivée lorsque son seuil de rétention est atteint, Amazon Data Lifecycle Manager désenregistre l'AMI et supprime les instantanés associés.
- Si vous désactivez une AMI créée par Amazon Data Lifecycle Manager et que vous archivez manuellement les instantanés associés, et que ces instantanés sont archivés lorsque leur seuil de rétention est atteint, Amazon Data Lifecycle Manager ne supprimera pas ces instantanés et ne les gèrera plus.

Les considérations suivantes s'appliquent aux politiques AMI et à la protection contre la désinscription des [AMI](#) :

- Si vous activez manuellement la protection contre le désenregistrement pour une AMI créée par Amazon Data Lifecycle Manager et qu'elle est toujours activée lorsque le seuil de rétention de l'AMI est atteint, Amazon Data Lifecycle Manager ne gère plus cette AMI. Vous devez désenregistrer manuellement l'AMI et supprimer ses instantanés sous-jacents s'il n'est plus nécessaire.

Ressources supplémentaires

Pour plus d'informations, consultez le blog [Automatiser la gestion des snapshots Amazon EBS et des AMI à l'aide du](#) AWS stockage Amazon Data Lifecycle Manager.

Automatisez les copies de snapshots entre comptes avec Data Lifecycle Manager

L'automatisation des copies d'instantanés entre comptes vous permet de copier vos instantanés Amazon EBS vers des régions spécifiques dans un compte isolé et de chiffrer ces instantanés à l'aide d'une clé de chiffrement. Cela vous permet de vous protéger contre la perte de données en cas de compromission de votre compte.

L'automatisation des copies d'instantanés entre comptes implique deux comptes :

- **Compte source** : le compte source est le compte qui crée et partage les instantanés avec le compte cible. Dans ce compte, vous devez créer une politique de capture d'écran EBS qui crée des instantanés à des intervalles définis, puis les partage avec d'autres AWS comptes.
- **Compte cible** : le compte cible est le compte avec le compte de destination avec lequel les instantanés sont partagés, et qui crée des copies des instantanés partagés. Dans ce compte, vous devez créer une politique d'événement de copie entre comptes qui copie automatiquement les instantanés qui sont partagés avec lui par un ou plusieurs comptes source spécifiés.

Note

La politique de capture d'écran EBS du compte source et la politique relative aux événements de copie entre comptes du compte cible doivent être créées dans la même AWS région. Le compte cible peut ensuite copier des instantanés vers différentes régions de destination selon les besoins.

Rubriques

- [Créer des politiques de copie d'instantané entre comptes](#)
- [Spécifier les filtres de description d'instantané](#)
- [Remarques relatives aux stratégies de copie d'instantané entre comptes](#)
- [Ressources supplémentaires](#)

Créer des politiques de copie d'instantané entre comptes

Pour préparer les comptes source et cible pour la copie des instantanés entre comptes, vous devez procéder comme suit :

Étape 1 : Création de la politique de capture instantanée EBS (Compte source)

Dans le compte source, créez une politique d'instantanés EBS qui créera les instantanés et partagera ceux-ci avec les comptes cibles requis.

Lorsque vous créez la politique, assurez-vous d'activer le partage entre comptes et de spécifier les AWS comptes cibles avec lesquels partager les instantanés. Il s'agit des comptes avec lesquels les instantanés doivent être partagés. Si vous partagez des instantanés chiffrés, vous devez accorder aux comptes cibles sélectionnés l'autorisation d'utiliser la clé KMS utilisée pour chiffrer le volume source. Pour de plus amples informations, veuillez consulter [Étape 2 : partager la clé gérée par le client \(Compte source\)](#).

Note

- Créez cette politique dans la même AWS région que celle où vous allez créer la politique relative aux événements de copie entre comptes du compte cible à l'étape 3. Les deux politiques doivent être appliquées dans la même région pour que le partage d'instantanés entre comptes fonctionne correctement.
- Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être partagés. Vous ne pouvez pas partager d'instantanés chiffrés à l'aide de la clé KMS de chiffrement EBS par défaut. Si vous partagez des instantanés chiffrés, vous devez également partager la clé KMS utilisée pour chiffrer le volume source avec les comptes cibles. Pour plus d'informations, consultez [Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS](#) dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur la création d'une politique d'instantané EBS, consultez [Création d'une politique personnalisée Amazon Data Lifecycle Manager pour les instantanés EBS](#).

Utilisez l'une des méthodes suivantes pour créer la politique d'instantanés EBS.

Étape 2 : partager la clé gérée par le client (Compte source)

Si vous partagez des instantanés chiffrés, vous devez accorder au rôle IAM et aux comptes AWS cibles (que vous avez sélectionnés à l'étape précédente) les autorisations d'utiliser la clé gérée par le client utilisée pour chiffrer le volume source.

Note

Ne suivez cette étape que si vous partagez des instantanés chiffrés. Si vous partagez des instantanés non chiffrés, ignorez cette étape.

Console

1. Ouvrez la AWS KMS console à l'adresse <https://console.aws.amazon.com/kms>.
2. Pour modifier la Région AWS, utilisez le sélecteur de région situé dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Clés gérées par le client, puis sélectionnez la clé CMK à partager avec les comptes cibles.

Prenez note de l'ARN de la clé KMS, car vous aurez besoin de celui-ci plus tard.

4. Sous l'onglet Stratégie de clé, faites défiler la page jusqu'à la section Utilisateurs de clé. Sélectionnez Ajouter, saisissez le nom du rôle IAM sélectionné à l'étape précédente, puis sélectionnez Ajouter.
5. Sous l'onglet Stratégie de clé, faites défiler la page jusqu'à la section Autres comptes AWS . Choisissez Ajouter d'autres AWS comptes, puis ajoutez tous les AWS comptes cibles avec lesquels vous avez choisi de partager les instantanés à l'étape précédente.
6. Sélectionnez Save Changes.

Command line

Utilisez la commande [get-key-policy](#) pour récupérer la stratégie de clé actuellement attachée à la clé KMS.

Par exemple, la commande suivante récupère la stratégie d'une clé KMS présentant l'ID 9d5e2b3d-e410-4a27-a958-19e220d83a1e et l'écrit dans un fichier nommé `snapshotKey.json`.

```
$ aws kms get-key-policy \
  --policy-name default \
  --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
  --query Policy \
  --output text > snapshotKey.json
```

Ouvrez la politique de clé à l'aide de l'éditeur de texte de votre choix. Ajoutez l'ARN du rôle IAM que vous avez spécifié lors de la création de la politique d'instantané et les ARN des comptes cibles avec lesquels partager la clé KMS.

Par exemple, dans la politique suivante, l'ARN du rôle IAM par défaut est spécifié, ainsi que l'ARN du compte racine du compte cible 222222222222.

Tip

Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour permettre à l'utilisateur de créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée pour le compte de l'utilisateur par un AWS service, comme illustré dans l'exemple suivant.

```
{
  "Sid" : "Allow use of the key",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : [
      "arn:aws:iam::111111111111:role/service-role/AWSDataLifecycleManagerDefaultRole",
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action" : [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource" : "*"
}
```

```

},
{
  "Sid" : "Allow attachment of persistent resources",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : [
      "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action" : [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource" : "*",
  "Condition" : {
    "Bool" : {
      "kms:GrantIsForAWSResource" : "true"
    }
  }
}
}

```

Enregistrez et fermez le fichier. Utilisez ensuite la commande [put-key-policy](#) pour attacher la stratégie de clé mise à jour à la clé KMS.

```

$ aws kms put-key-policy \
  --policy-name default \
  --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
  --policy file://snapshotKey.json

```

Étape 3 : Création d'une politique relative aux événements de copie entre comptes (Compte cible)

Dans le compte cible, vous devez créer une politique d'événement de copie entre comptes qui copiera automatiquement les instantanés partagés par les comptes source requis.

Cette politique s'exécute uniquement dans le compte cible lorsque l'un des comptes sources spécifiés partage l'instantané avec le compte.

 Note

Créez cette politique dans la même AWS région que la politique de capture instantanée EBS du compte source créée à l'étape 1. Les deux politiques doivent être appliquées dans la même région pour que le partage d'instantanés entre comptes fonctionne correctement. Vous pouvez ensuite configurer cette politique pour copier les instantanés vers différentes régions de destination selon vos besoins.

Utilisez l'une des méthodes suivantes pour créer la politique d'événement de copie entre comptes.

Console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Sur l'écran Sélectionner le type de politique, choisissez Cross-account Copier la politique des événements, puis choisissez Suivant.
4. Pour Description de la stratégie, entrez une brève description de la stratégie.
5. Pour Etiquettes de stratégie, ajoutez les étiquettes à appliquer à la stratégie de cycle de vie. Vous pouvez utiliser ces étiquettes pour identifier et catégoriser vos politiques.
6. Dans la section Paramètres de l'événement, définissez l'événement de partage d'instantané qui entraînera l'exécution de la stratégie. Procédez comme suit :
 - a. Pour les comptes de partage, spécifiez les AWS comptes sources à partir desquels vous souhaitez copier les instantanés partagés. Choisissez Ajouter un compte, entrez l'identifiant de AWS compte à 12 chiffres, puis choisissez Ajouter.
 - b. Pour Filtrer par description, saisissez la description d'instantané requise en utilisant une expression régulière. Seuls les instantanés partagés par les comptes sources spécifiés et dont les descriptions correspondent au filtre spécifié sont copiés par la politique. Pour plus d'informations, consultez [Spécifier les filtres de description d'instantané](#).
7. Pour le rôle IAM, sélectionnez le rôle IAM autorisé à effectuer des actions de copie d'instantané. Pour utiliser le rôle par défaut fourni par Amazon Data Lifecycle Manager, choisissez Rôle par défaut. Autrement, pour utiliser un rôle IAM personnalisé que vous avez créé précédemment, sélectionnez Choisir un autre rôle, puis sélectionnez le rôle à utiliser.

Si vous copiez des instantanés chiffrés, vous devez accorder au rôle IAM sélectionné les autorisations nécessaires pour utiliser la clé de chiffrement clé KMS utilisée pour chiffrer le volume source. De même, si vous chiffrez l'instantané dans la région de destination à l'aide d'une autre clé KMS, vous devez accorder au rôle IAM l'autorisation d'utiliser la clé KMS de destination. Pour plus d'informations, consultez [Étape 4 : Autoriser le rôle IAM à utiliser les clés KMS requises \(Compte cible\)](#).

8. Dans la section Copier une action, définissez les actions de copie d'instantané que la stratégie doit exécuter quand elle est activée. La politique peut copier des instantanés vers jusqu'à trois régions. Vous devez spécifier une règle de copie distincte pour chaque région de destination. Pour chaque règle que vous ajoutez, procédez comme suit :
 - a. Pour Nom, saisissez un nom descriptif pour la copie.
 - b. Pour Région cible, sélectionnez la région dans laquelle copier les instantanés.
 - c. Pour Expirer, spécifiez la durée de rétention des copies d'instantané dans la région cible après leur création.
 - d. Pour chiffrer la copie d'instantané, pour Chiffrement, sélectionnez Activer le chiffrement. Si l'instantané source est chiffré ou si le chiffrement par défaut est activé pour votre compte, alors la copie d'instantané est toujours chiffrée, même si vous n'activez pas le chiffrement ici. Si l'instantané source n'est pas chiffré et que le chiffrement par défaut n'est pas activé pour votre compte, vous pouvez choisir d'activer ou de désactiver le chiffrement. Si vous activez le chiffrement, mais que vous ne spécifiez pas de clé KMS, les instantanés sont chiffrés à l'aide de la clé KMS de chiffrement par défaut dans chaque région de destination. Si vous spécifiez une clé KMS pour la région de destination, vous devez avoir accès à la clé KMS.
9. Pour ajouter des actions de copie d'instantané, choisissez Ajouter de nouvelles régions.
10. Pour Policy status after creation (Statut de la stratégie après création), choisissez Enable policy (Activer la stratégie) pour lancer les exécutions de stratégie lors de la prochaine heure planifiée ou Disable policy (Désactiver la stratégie) pour empêcher l'exécution de la stratégie. Si vous n'activez pas la politique maintenant, elle ne commencera à copier des instantanés que quand vous l'aurez activée manuellement après sa création.
11. Choisissez Créer une stratégie.

Command line

Utilisez la commande [create-lifecycle-policy](#) pour créer une stratégie. Pour créer une stratégie d'événement de copie entre comptes, pour PolicyType, spécifiez EVENT_BASED_POLICY.

Par exemple, la commande suivante crée une stratégie d'événement de copie entre comptes dans le compte cible 222222222222. La stratégie copie les instantanés qui sont partagés par le compte source 111111111111. La stratégie copie les instantanés vers sa-east-1 et eu-west-2. Les instantanés copiés vers sa-east-1 ne sont pas chiffrés et sont retenus pendant 3 jours. Les instantanés copiés vers eu-west-2 sont chiffrés à l'aide de la clé 8af79514-350d-4c52-bac8-8985e84171c7 clé KMS et sont conservés pendant 1 mois. La politique utilise le rôle IAM par défaut.

```
$ aws dlm create-lifecycle-policy \
  --description "Copy policy" \
  --state ENABLED \
  --execution-role-arn arn:aws:iam::222222222222:role/service-role/
  AWSDataLifecycleManagerDefaultRole \
  --policy-details file://policyDetails.json
```

L'exemple suivant affiche le contenu du fichier policyDetails.json.

```
{
  "PolicyType" : "EVENT_BASED_POLICY",
  "EventSource" : {
    "Type" : "MANAGED_CWE",
    "Parameters": {
      "EventType" : "shareSnapshot",
      "SnapshotOwner": ["111111111111"]
    }
  },
  "Actions" : [{
    "Name" : "Copy Snapshot to Sao Paulo and London",
    "CrossRegionCopy" : [{
      "Target" : "sa-east-1",
      "EncryptionConfiguration" : {
        "Encrypted" : false
      },
      "RetainRule" : {
        "Interval" : 3,
        "IntervalUnit" : "DAYS"
      }
    }
  ]
}
```

```

    },
    {
      "Target" : "eu-west-2",
      "EncryptionConfiguration" : {
        "Encrypted" : true,
        "CmkArn" : "arn:aws:kms:eu-west-2:222222222222:key/8af79514-350d-4c52-bac8-8985e84171c7"
      },
      "RetainRule" : {
        "Interval" : 1,
        "IntervalUnit" : "MONTHS"
      }
    }
  ]
}

```

Si la demande aboutit, la commande renvoie l’ID de la politique nouvellement créée. Voici un exemple de sortie.

```

{
  "PolicyId": "policy-9876543210abcdef0"
}

```

Étape 4 : Autoriser le rôle IAM à utiliser les clés KMS requises (Compte cible)

Si vous copiez des instantanés chiffrés, vous devez accorder au rôle IAM (que vous avez sélectionné à l’étape précédente) les autorisations d’utiliser la clé gérée par le client utilisée pour chiffrer le volume source.

Note

Suivez cette étape uniquement si vous copiez des instantanés chiffrés. Si vous copiez des instantanés non chiffrés, ignorez cette étape.

Utilisez l’une des méthodes suivantes pour ajouter les politiques requises au rôle IAM.

Console

1. Ouvrez la console IAM à l’adresse <https://console.aws.amazon.com/iam/>.

2. Dans le volet de navigation, sélectionnez Rôles. Recherchez et sélectionnez le rôle IAM que vous avez sélectionné lors de la création de la politique d'événement de copie entre comptes à l'étape précédente. Si vous avez choisi d'utiliser le rôle par défaut, celui-ci est nommé `AWSDatalifecycleManagerDefaultRole`.
3. Sélectionnez Ajouter une stratégie en ligne, puis l'onglet JSON.
4. Remplacez la politique existante par ce qui suit et spécifiez l'ARN de clé KMS qui a été utilisé pour chiffrer les volumes sources et qui a été partagé avec vous par le compte source à l'étape 2.

 Note

Si vous copiez à partir de plusieurs comptes sources, vous devez spécifier l'ARN de clé KMS correspondant à partir de chaque compte source.

Dans l'exemple suivant, la stratégie accorde au rôle IAM l'autorisation d'utiliser la clé 1234abcd-12ab-34cd-56ef-1234567890ab clé KMS, qui a été partagée par le compte source 111111111111, et la clé 4567dcba-23ab-34cd-56ef-0987654321yz clé KMS, qui existe dans le compte cible 222222222222.

 Tip

Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour permettre à l'utilisateur de créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée pour le compte de l'utilisateur par un AWS service, comme illustré dans l'exemple suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

        "kms:RevokeGrant",
        "kms:CreateGrant",
        "kms:ListGrants"
    ],
    "Resource": [
        "arn:aws:kms:us-east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
    ],
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": [
        "arn:aws:kms:us-east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
    ]
}
]
}

```

5. Choisissez Review policy (Examiner la politique)
6. Dans Nom, saisissez un nom descriptif pour la stratégie, puis sélectionnez Créer une stratégie.

Command line

À l'aide de l'éditeur de texte de votre choix, créez un fichier JSON nommé `policyDetails.json`. Ajoutez la politique suivante et spécifiez l'ARN de clé KMS qui a été utilisé pour chiffrer les volumes sources et qui a été partagé avec vous par le compte source à l'étape 2.

Note

Si vous copiez à partir de plusieurs comptes sources, vous devez spécifier l'ARN de clé KMS correspondant à partir de chaque compte source.

Dans l'exemple suivant, la stratégie accorde au rôle IAM l'autorisation d'utiliser la clé 1234abcd-12ab-34cd-56ef-1234567890ab clé KMS, qui a été partagée par le compte source 111111111111, et la clé 4567dcba-23ab-34cd-56ef-0987654321yz clé KMS, qui existe dans le compte cible 222222222222.

Tip

Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour permettre à l'utilisateur de créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée pour le compte de l'utilisateur par un AWS service, comme illustré dans l'exemple suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:RevokeGrant",
        "kms:CreateGrant",
        "kms:ListGrants"
      ]
    }
  ]
}
```

```

    ],
    "Resource": [
        "arn:aws:kms:us-  
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-  
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
    ],
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": [
        "arn:aws:kms:us-  
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "arn:aws:kms:us-  
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
    ]
}
]
}

```

Enregistrez et fermez le fichier . Utilisez ensuite la commande [put-role-policy](#) pour ajouter la stratégie au rôle IAM.

Par exemple

```

$ aws iam put-role-policy \
  --role-name AWSDataLifecycleManagerDefaultRole \
  --policy-name CopyPolicy \
  --policy-document file://AdminPolicy.json

```

Spécifier les filtres de description d'instantané

Lorsque vous créez la politique de copie de cliché dans le compte cible, vous devez spécifier un filtre de description d'instantané. Le filtre de description d'instantané vous permet de spécifier un niveau de filtrage supplémentaire qui vous permet de contrôler quels instantanés sont copiés par la politique. Cela signifie qu'un instantané n'est copié par la politique que s'il est partagé par l'un des comptes source spécifiés et qu'il possède une description d'instantané qui correspond au filtre spécifié. En d'autres termes, si un instantané est partagé par l'un des comptes de cours spécifiés, mais qu'il n'a pas de description correspondant au filtre spécifié, il n'est pas copié par la politique.

La description du filtre d'instantané doit être spécifiée à l'aide d'une expression régulière. Il s'agit d'un champ obligatoire lors de la création de politiques d'événement de copie entre comptes à l'aide de la console et de la ligne de commande. Voici des exemples d'expressions régulières qui peuvent être utilisées :

- `.*` : ce filtre correspond à toutes les descriptions des instantanés. Si vous utilisez cette expression, la politique copiera tous les instantanés partagés par l'un des comptes source spécifiés.
- `Created for policy: policy-0123456789abcdef0.*`—ce filtre ne correspond qu'aux instantanés créés par une stratégie dont l'ID est de `policy-0123456789abcdef0`. Si vous utilisez une expression comme celle-ci, seuls les instantanés partagés avec votre compte par l'un des comptes source spécifiés et qui ont été créés par une politique avec l'ID spécifié sont copiés par la politique.
- `.*production.*` : ce filtre correspond à n'importe quel instantané dont le mot `production` est indiqué n'importe où dans sa description. Si vous utilisez cette expression, la politique copiera tous les instantanés partagés par l'un des comptes source spécifiés et dont la description contient le texte spécifié.

Remarques relatives aux stratégies de copie d'instantané entre comptes

Les considérations suivantes s'appliquent aux politiques d'événement de copie entre comptes :

- La politique de capture d'écran EBS du compte source et la politique relative aux événements de copie entre comptes du compte cible doivent être créées dans la même AWS région. Une fois l'instantané partagé, la politique du compte cible peut copier l'instantané vers différentes régions de destination, comme indiqué dans les actions de copie.
- Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être copiés.

- Vous pouvez créer une politique d'événement de copie entre comptes pour copier les instantanés partagés en dehors de Amazon Data Lifecycle Manager.
- Si vous souhaitez chiffrer les instantanés dans le compte cible, le rôle IAM sélectionné pour la politique d'événement de copie entre comptes doit être autorisé à utiliser la clé KMS requise.

Ressources supplémentaires

Pour plus d'informations, consultez le blog [Automatisation de la copie des instantanés Amazon EBS chiffrés entre les AWS comptes](#) AWS et le stockage.

Modifier les politiques d'Amazon Data Lifecycle Manager

Gardez les points suivants à l'esprit lorsque vous modifiez les politiques d'Amazon Data Lifecycle Manager :

- Si vous modifiez une politique d'AMI ou d'instantané en supprimant ou en modifiant ses identifications cible, les volumes ou les instances de ces identifications ne sont plus gérées par la politique.
- Si vous modifiez le nom de la planification, les instantanés ou les AMI créées sous l'ancien nom de planification ne sont plus gérées par la politique.
- Si vous modifiez une planification de rétention basée sur l'âge pour utiliser un nouvel intervalle, ce dernier est utilisé uniquement pour les nouveaux instantanés ou AMI créées après la modification. Le nouveau programme n'affecte pas la planification de rétention des instantanés ou des AMI créés avant la modification.
- Vous ne pouvez pas modifier la planification de rétention d'une politique en passant d'une politique basée sur le nombre à une politique basée sur l'âge après la création de celle-ci. Pour pouvoir effectuer ce changement, vous devez créer une nouvelle politique.
- Si vous désactivez une politique avec une planification de rétention basée sur l'âge, les instantanés ou les AMI qui sont définis pour expirer pendant que la politique est désactivée sont conservés indéfiniment. Vous devez supprimer les instantanés ou désenregistrer manuellement les AMI. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la suppression des instantanés ou désenregistrer les AMI à mesure que leurs périodes de rétention expirent.
- Si vous désactivez une politique avec un programme de rétention basé sur le comptage, la politique arrête de créer et de supprimer des instantanés ou des AMI. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la création d'instantanés et d'AMI, ainsi que la suppression d'instantanés ou d'AMI lorsque le seuil de rétention est atteint.

- Si vous désactivez une politique pour laquelle l'archivage des instantanés est activé, les instantanés qui se trouvent dans le niveau d'archivage au moment de la désactivation de la politique ne sont plus gérés par Amazon Data Lifecycle Manager. Vous devez supprimer l'instantané manuellement lorsqu'il n'est plus nécessaire.
- Si vous activez l'archivage des instantanés selon une planification basée sur le nombre, la règle d'archivage s'applique à tous les nouveaux instantanés créés et archivés selon la planification, ainsi qu'aux instantanés existants qui ont été précédemment créés et archivés selon la planification.
- Si vous activez l'archivage des instantanés selon une planification basée sur l'âge, la règle d'archivage s'applique uniquement aux nouveaux instantanés créés après activation de l'archivage des instantanés. Les instantanés existants créés avant l'activation de l'archivage des instantanés continuent d'être supprimés de leurs niveaux de stockage respectifs, conformément à la planification définie lors de leur création et de leur archivage initiaux.
- Si vous désactivez l'archivage des instantanés d'une planification basée sur le nombre, la planification arrête immédiatement l'archivage des instantanés. Les instantanés précédemment archivés selon la planification restent dans le niveau d'archivage et ne seront pas supprimés par Amazon Data Lifecycle Manager.
- Si vous désactivez l'archivage des instantanés d'une planification basée sur l'âge, les instantanés créés par la politique et dont l'archivage est prévu sont définitivement supprimés à la date et à l'heure d'archivage planifiées, comme indiqué par la balise système `aws:dlm:expirationTime`.
- Si vous désactivez l'archivage des instantanés d'une planification, la planification arrête immédiatement l'archivage des instantanés. Les instantanés précédemment archivés selon la planification restent dans le niveau d'archivage et ne seront pas supprimés par Amazon Data Lifecycle Manager.
- Si vous modifiez le nombre de rétention d'archivage pour une planification basée sur le nombre, le nouveau nombre de rétention inclut les instantanés existants qui étaient précédemment archivés selon la planification.
- Si vous modifiez la période de rétention d'archivage selon une planification basée sur l'âge, la nouvelle période de rétention s'applique uniquement aux instantanés archivés après modification de la règle de rétention.

Utilisez l'une des procédures suivantes pour modifier une politique de cycle de vie.

Console

Pour modifier une politique de cycle de vie

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Elastic Block Store, Lifecycle Manager (Gestionnaire de cycle de vie).
3. Sélectionnez une politique de cycle de vie dans la liste.
4. Sélectionnez Actions, puis Modifier une stratégie de cycle de vie.
5. Modifiez les paramètres de politique selon vos besoins. Par exemple, vous pouvez modifier le programme, ajouter ou supprimer des balises, ou encore activer ou désactiver la politique.
6. Choisissez Modifier la stratégie.

Command line

Utilisez la commande [update-lifecycle-policy](#) pour modifier les informations dans une stratégie de cycle de vie. Pour simplifier la syntaxe, cet exemple fait référence à un fichier JSON, `policyDetailsUpdated.json`, qui inclut les détails de la stratégie.

```
aws dlm update-lifecycle-policy \
  --state DISABLED \
  --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
  --policy-details file://policyDetailsUpdated.json
```

Voici un exemple du fichier `policyDetailsUpdated.json`.

```
{
  "ResourceTypes": [
    "VOLUME"
  ],
  "TargetTags": [
    {
      "Key": "costcenter",
      "Value": "120"
    }
  ],
  "Schedules": [
    {
```

```

    "Name": "DailySnapshots",
    "TagsToAdd": [
      {
        "Key": "type",
        "Value": "myDailySnapshot"
      }
    ],
    "CreateRule": {
      "Interval": 12,
      "IntervalUnit": "HOURS",
      "Times": [
        "15:00"
      ]
    },
    "RetainRule": {
      "Count": 5
    },
    "CopyTags": false
  }
]
}

```

Pour afficher la stratégie mise à jour, utilisez la commande `get-lifecycle-policy`. Vous pouvez voir que l'état, la valeur de la balise, l'intervalle de prise d'instantané et l'heure de début de la prise d'instantané ont été modifiés.

Supprimer les politiques d'Amazon Data Lifecycle Manager

Lorsque vous supprimez des politiques Amazon Data Lifecycle Manager, tenez compte des points suivants :

- Si vous supprimez une politique, les instantanés ou les AMI créés par cette politique ne sont pas automatiquement supprimés. Si vous n'avez plus besoin des instantanés ou des AMI, vous devez les supprimer manuellement.
- Si vous supprimez une politique pour laquelle l'archivage des instantanés est activé, les instantanés qui se trouvent dans le niveau d'archivage au moment de la suppression de la politique ne sont plus gérés par Amazon Data Lifecycle Manager. Vous devez supprimer l'instantané manuellement lorsqu'il n'est plus nécessaire.
- Si vous supprimez une politique avec une planification basée sur l'archivage et sur l'âge, les instantanés créés par la politique et dont l'archivage est prévu sont définitivement

supprimés à la date et à l'heure d'archivage planifiées, comme indiqué par la balise système `aws:dlm:expirationtime`.

Utilisez l'une des procédures suivantes pour supprimer une politique de cycle de vie.

Console

Pour supprimer une politique de cycle de vie

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, choisissez Elastic Block Store, Lifecycle Manager (Gestionnaire de cycle de vie).
3. Sélectionnez une politique de cycle de vie dans la liste.
4. Sélectionnez Actions, puis Supprimer une stratégie de cycle de vie.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer une stratégie de cycle de vie.

Command line

Utilisez la commande [delete-lifecycle-policy](#) pour supprimer une stratégie de cycle de vie et libérer les balises cible spécifiées dans la stratégie afin de pouvoir les réutiliser.

Note

Vous pouvez supprimer les instantanés créés uniquement par Amazon Data Lifecycle Manager.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Le manuel [Référence d'API Amazon Data Lifecycle Manager](#) contient des descriptions et la syntaxe de chacune des actions et chacun des types de données de l'API de requête Amazon Data Lifecycle Manager.

Vous pouvez également utiliser l'un des AWS SDK pour accéder à l'API d'une manière adaptée au langage de programmation ou à la plateforme que vous utilisez. Pour plus d'informations, consultez [Kits SDK AWS](#).

Contrôlez l'accès à Amazon Data Lifecycle Manager à l'aide d'IAM

Des informations d'identification sont nécessaires pour accéder à Amazon Data Lifecycle Manager. Ces informations d'identification doivent avoir les autorisations pour accéder aux ressources AWS, telles que les instances, les volumes, les instantanés et les AML.

Les autorisations IAM suivantes sont requises pour utiliser Amazon Data Lifecycle Manager.

Note

- Les autorisations `ec2:DescribeAvailabilityZones`, `ec2:DescribeRegions`, `kms:ListAliases` et `kms:DescribeKey` sont nécessaires pour les utilisateurs de la console uniquement. Si l'accès à la console n'est pas requis, vous pouvez supprimer les autorisations.
- Le format ARN du `AWSDataLifecycleManagerDefaultRole` rôle diffère selon qu'il a été créé à l'aide de la console ou du AWS CLI. Si le rôle a été créé à l'aide de la console, le format ARN est `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`. Si le rôle a été créé à l'aide du AWS CLI, le format ARN est `arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "dlm:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```

        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::111122223333:role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::111122223333:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement",
            "arn:aws:iam::111122223333:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::111122223333:role/service-role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement"
        ]
    },
    {
        "Effect": "Allow",
        "Action": "iam:ListRoles",
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeRegions",
            "kms:ListAliases",
            "kms:DescribeKey"
        ],
        "Resource": "*"
    }
]
}

```

Autorisations pour le chiffrement

Tenez compte des éléments suivants lorsque vous travaillez avec Amazon Data Lifecycle Manager et des ressources chiffrées.

- Si le volume source est chiffré, assurez-vous que les rôles par défaut d'Amazon Data Lifecycle Manager (AWSDataLifecycleManagerDefaultRole et AWSDataLifecycleManagerDefaultRoleForAMIManagement) sont autorisés à utiliser les clés KMS utilisées pour chiffrer le volume.
- Si vous activez la copie entre régions pour les instantanés non chiffrés ou les AMI sauvegardées par des instantanés non chiffrés, et que vous choisissez d'activer le chiffrement dans la région de

destination, assurez-vous que les rôles par défaut sont autorisés à utiliser la clé KMS nécessaire pour effectuer le chiffrement dans la région de destination.

- Si vous activez la copie entre régions pour les instantanés chiffrés ou les AMI sauvegardées par des instantanés chiffrés, assurez-vous que les rôles par défaut sont autorisés à utiliser à la fois les clés KMS source et de destination.
- Si vous activez l'archivage des instantanés pour les instantanés chiffrés, assurez-vous que le rôle par défaut d'Amazon Data Lifecycle Manager (`AWSDatalifecycleManagerDefaultRole`) est autorisé à utiliser la clé KMS utilisée pour chiffrer l'instantané.

Pour plus d'informations, consultez [Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS](#) dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations, consultez [Modification des autorisations d'un utilisateur](#) dans le Guide de l'utilisateur IAM.

AWS politiques gérées pour Amazon Data Lifecycle Manager

Une politique AWS gérée est une politique autonome qui est créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants. AWS les politiques gérées vous permettent d'attribuer les autorisations appropriées aux utilisateurs, aux groupes et aux rôles de manière plus efficace que si vous deviez rédiger les politiques vous-même.

Cependant, vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. AWS met occasionnellement à jour les autorisations définies dans une politique AWS gérée. Dans ce cas, la mise à jour affecte toutes les entités de principaux (utilisateurs, groupes et rôles) auxquelles la politique est attachée.

Amazon Data Lifecycle Manager fournit des politiques AWS gérées pour les cas d'utilisation courants. Ces politiques facilitent la définition des autorisations appropriées et le contrôle de l'accès à vos ressources. Les politiques AWS gérées fournies par Amazon Data Lifecycle Manager sont conçues pour être associées aux rôles que vous transmettez à Amazon Data Lifecycle Manager.

Rubriques

- [AWSDatalifecycleManagerServiceRole](#)
- [AWSDatalifecycleManagerServiceRoleForAMIManagement](#)
- [AWSDatalifecycleManagerSSMFullAccess](#)

- [AWS mises à jour des politiques gérées](#)

AWSDatalifecycleManagerServiceRole

La `AWSDatalifecycleManagerServiceRole` politique fournit les autorisations appropriées à Amazon Data Lifecycle Manager pour créer et gérer les politiques relatives aux instantanés Amazon EBS et les politiques relatives aux événements de copie entre comptes.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    }
  ]
}
```



```

        "Effect": "Allow",
        "Action": [
            "events:PutRule",
            "events>DeleteRule",
            "events:DescribeRule",
            "events:EnableRule",
            "events:DisableRule",
            "events:ListTargetsByRule",
            "events:PutTargets",
            "events:RemoveTargets"
        ],
        "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-
cwe.*"
    }
]
}

```

AWSDataLifecycleManagerServiceRoleForAMIManagement

La `AWSDataLifecycleManagerServiceRoleForAMIManagement` politique fournit les autorisations appropriées à Amazon Data Lifecycle Manager pour créer et gérer les politiques Amazon EBS-backed AMI.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",

```

```

        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:ResetImageAttribute",
      "ec2:DeregisterImage",
      "ec2:CreateImage",
      "ec2:CopyImage",
      "ec2:ModifyImageAttribute"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:EnableImageDeprecation",
      "ec2:DisableImageDeprecation"
    ],
    "Resource": "arn:aws:ec2:*::image/*"
  }
]
}

```

AWSDataLifecycleManagerSSMFullAccess

Fournit à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions Systems Manager requises pour exécuter des pré-scripts et des post-scripts sur toutes les instances Amazon EC2.

Important

La politique utilise la clé de condition `aws:ResourceTag` pour restreindre l'accès à des documents SSM spécifiques lors de l'utilisation de pré-scripts et de post-scripts. Pour

permettre à Amazon Data Lifecycle Manager d'accéder aux documents SSM, vous devez vous assurer que vos documents SSM sont balisés avec `DLMScriptsAccess:true`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSMReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowTaggedSSMDocumentsOnly",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/DLMScriptsAccess": "true"
        }
      }
    },
    {
      "Sid": "AllowSpecificAWSOwnedSSMDocuments",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
```

```

        "ssm:GetDocument"
    ],
    "Resource": [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
    ]
},
{
    "Sid": "AllowAllEC2Instances",
    "Effect": "Allow",
    "Action": [
        "ssm:SendCommand"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

AWS mises à jour des politiques gérées

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 parfois des autorisations supplémentaires à une politique AWS gérée 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 AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations deviennent disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée, de sorte que les mises à jour des politiques n'annuleront pas vos autorisations existantes.

Le tableau suivant fournit des informations sur les mises à jour des politiques AWS gérées pour Amazon Data Lifecycle Manager depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS de la page [Historique des documents pour le guide de l'utilisateur Amazon EBS](#).

Modifier	Description	Date
AWSDatalifecycleManagerServiceRole— Mise à jour des autorisations de la politique.	Amazon Data Lifecycle Manager a ajouté l'ec2:DescribeAvailabilityZones action permettant d'autoriser les politiques de capture instantanée à obtenir des informations sur les zones locales.	16 décembre 2024
AWSDatalifecycleManagerSSMFullAccess— Mise à jour des autorisations de la politique.	Mise à jour de la politique afin de prendre en charge les instantanés cohérents par rapport à l'application pour SAP HANA à l'aide du document SSM AWSSystemsManagerSAP-CreateDLMSnapshotForSAPANA .	17 novembre 2023

Modifier	Description	Date
AWSDatalifecycleManagerSSMFullAccess— Ajout d'une nouvelle politique AWS gérée.	Amazon Data Lifecycle Manager a ajouté la politique AWSDatalifecycleManagerSSMFullAccess AWS gérée.	7 novembre 2023
AWSDatalifecycleManagerServiceRole— Ajout d'autorisations pour prendre en charge l'archivage des instantanés.	Amazon Data Lifecycle Manager a ajouté les actions <code>ec2:ModifySnapshotTier</code> et <code>ec2:DescribeSnapshotTierStatus</code> visant à accorder aux politiques d'instantanés l'autorisation d'archiver des instantanés et de vérifier l'état d'archivage des instantanés.	30 septembre 2022

Modifier	Description	Date
AWSDataLifecycleManagerServiceRoleForAMIManagement— Ajout d'autorisations pour prendre en charge la dépréciation des AMI.	Amazon Data Lifecycle Manager a ajouté les <code>ec2:DisableImageDeprecation</code> et <code>ec2:EnableImageDeprecation</code> pour accorder aux politiques EBS-backup d'AMI l'autorisation d'activer et de désactiver la dépréciation des AMI.	23 août 2021
Début du suivi des modifications par Amazon Data Lifecycle Manager	Amazon Data Lifecycle Manager a commencé à suivre les modifications apportées AWS à ses politiques gérées.	23 août 2021

Rôles de service IAM pour Amazon Data Lifecycle Manager

Un rôle Gestion des identités et des accès AWS (IAM) est similaire à celui d'un utilisateur, dans la mesure où il s'agit d'une AWS identité dotée de politiques d'autorisations qui déterminent ce que

l'identité peut et ne peut pas faire. AWS En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être assumé par tout utilisateur qui en a besoin. Un rôle de service est un rôle assumé par un AWS service pour effectuer des actions en votre nom. Amazon Data Lifecycle Manager étant le service qui effectue des opérations de sauvegarde en votre nom, vous devez lui transmettre un rôle à assumer lorsqu'il effectue des opérations de politique en votre nom. Pour plus d'informations sur les rôles IAM, consultez [Rôles IAM](#) dans le Guide de l'utilisateur IAM.

Le rôle que vous transmettez à Amazon Data Lifecycle Manager doit disposer d'une politique IAM avec les autorisations qui permettent à Amazon Data Lifecycle Manager d'effectuer des actions associées aux opérations de politique, telles que la création d'instantanés et d'AMI, la copie d'instantanés et d'AMI, la suppression d'instantanés et la désinscription d'AMI. Chaque type de politique Amazon Data Lifecycle Manager nécessite des autorisations différentes. Amazon Data Lifecycle Manager doit également être répertorié comme entité approuvée par le rôle, ce qui permet à Amazon Data Lifecycle Manager d'assumer ce rôle.

Rubriques

- [Fonctions du service par défaut pour Amazon Data Lifecycle Manager](#)
- [Fonctions du service personnalisées pour Amazon Data Lifecycle Manager](#)

Fonctions du service par défaut pour Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager utilise les fonctions du service par défaut suivantes :

- **AWSDataLifecycleManagerDefaultRole**—rôle par défaut pour la gestion des instantanés. Il ne fait confiance qu'au service `d1m.amazonaws.com` pour assumer ce rôle et il permet à Amazon Data Lifecycle Manager d'effectuer en votre nom les actions requises par les politiques d'instantané et de copie d'instantané inter-comptes. Ce rôle utilise la politique **AWSDataLifecycleManagerServiceRole** AWS gérée.

Note

Le format ARN du rôle diffère selon qu'il a été créé à l'aide de la console ou de l'AWS CLI. Si le rôle a été créé à l'aide de la console, le format ARN est `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`. Si le rôle a été créé à l'aide

du AWS CLI, le format ARN est `arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`.

- `AWSDataLifecycleManagerDefaultRoleForAMIManagement`—rôle par défaut pour la gestion des AMI. Il ne fait confiance qu'au `d1m.amazonaws.com` service pour assumer le rôle et permet à Amazon Data Lifecycle Manager d'effectuer les actions requises par les politiques EBS-backed AMI en votre nom. Ce rôle utilise la politique `AWSDataLifecycleManagerServiceRoleForAMIManagement` AWS gérée.

Si vous utilisez la console Amazon Data Lifecycle Manager, Amazon Data Lifecycle Manager crée automatiquement le rôle de `AWSDataLifecycleManagerDefaultRole` service la première fois que vous créez un snapshot ou une politique de copie de snapshot entre comptes, et il crée automatiquement le rôle de `AWSDataLifecycleManagerDefaultRoleForAMIManagement` service la première fois que vous créez une politique EBS-backed AMI.

Si vous n'utilisez pas la console, vous pouvez créer manuellement les fonctions du service en utilisant la commande [create-default-role](#) (Créer un rôle par défaut). Pour `--resource-type`, spécifiez `snapshot` de créer `AWSDataLifecycleManagerDefaultRole` ou `image` de créer `AWSDataLifecycleManagerDefaultRoleForAMIManagement`.

```
$ aws dlm create-default-role --resource-type snapshot|image
```

Si vous supprimez les fonctions du service par défaut et que par la suite vous avez besoin de les recréer, vous pourrez utiliser la même procédure pour recréer les rôles dans votre compte.

Fonctions du service personnalisées pour Amazon Data Lifecycle Manager

Vous pouvez également choisir de créer des rôles IAM personnalisés possédant les autorisations requises et les sélectionner lors de la création d'une politique de cycle de vie, comme alternative aux fonctions du service par défaut.

Pour créer un rôle IAM personnalisé

1. Créez des rôles avec les autorisations suivantes.
 - Autorisations requises pour la gestion des politiques de cycle de vie des instantanés

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2>DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "events:PutRule",
        "events>DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",

```

```

        "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/
    AwsDataLifecycleRule.managed-cwe.*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:GetCommandInvocation",
      "ssm:ListCommands",
      "ssm:DescribeInstanceInformation"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:SendCommand",
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource": [
      "arn:aws:ssm:*:*:document/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/DLMScriptsAccess": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ssm:SendCommand",
      "ssm:DescribeDocument",
      "ssm:GetDocument"
    ],
    "Resource": [
      "arn:aws:ssm:*:*:document/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [

```

```

        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:ResourceTag/DLMScriptsAccess": "false"
        }
      }
    }
  ]
}

```

- Autorisations pour la gestion des politiques de cycle de vie des AMI

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteSnapshot",
      "Resource": "arn:aws:ec2:*:*:snapshot/*"
    }
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource": "arn:aws:ec2:*::image/*"
    }
  ]
}

```

Pour plus d'informations, consultez [Création d'un rôle](#) dans le IAM Guide de l'utilisateur.

2. Ajoutez une relation d'approbation aux rôles.
 - a. Dans la console IAM, choisissez Rôles.
 - b. Sélectionnez les rôles que vous avez créés, puis sélectionnez Trust relationships (Relations d'approbation).
 - c. Choisissez Modifier la relation d'approbation, ajoutez la stratégie suivante, puis choisissez Mettre à jour la stratégie d'approbation.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": "dlm.amazonaws.com"
    }
  }]
}

```

```
    },  
    "Action": "sts:AssumeRole"  
  }  
}
```

Nous vous recommandons d'utiliser les clés de condition `aws:SourceAccount` et `aws:SourceArn` pour vous protéger contre [le problème du député confus](#). Par exemple, vous pouvez ajouter le bloc de condition suivant à la stratégie d'approbation précédente. `aws:SourceAccount` est propriétaire de la politique de cycle de vie et `aws:SourceArn` est l'ARN de la politique de cycle de vie. Si vous ne connaissez pas l'ID de politique de cycle de vie, vous pouvez remplacer cette partie de l'ARN par un caractère générique (*), puis mettre à jour la politique d'approbation après avoir créé la politique de cycle de vie.

```
"Condition": {  
  "StringEquals": {  
    "aws:SourceAccount": "account_id"  
  },  
  "ArnLike": {  
    "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"  
  }  
}
```

Surveillez les politiques d'Amazon Data Lifecycle Manager

Vous pouvez utiliser les fonctions suivantes pour surveiller le cycle de vie de vos instantanés et vos AMI.

Caractéristiques

- [Console et AWS CLI](#)
- [Surveillez les politiques du Data Lifecycle Manager à l'aide de EventBridge](#)
- [Surveillez les politiques du Data Lifecycle Manager à l'aide de CloudWatch](#)
- [Journalisation des appels d'API Amazon Data Lifecycle Manager avec AWS CloudTrail](#)

Console et AWS CLI

Vous pouvez afficher vos politiques de cycle de vie à l'aide de la console Amazon EC2 ou d' AWS CLI. Chaque instantané et AMI créé par une politique possède un horodatage et des balises liées à la politique. Vous pouvez filtrer les instantanés et les AMI à l'aide de ces balises afin de vérifier que vos sauvegardes ont été créées comme vous le souhaitez.

Surveillez les politiques du Data Lifecycle Manager à l'aide de EventBridge

Amazon EBS et Amazon Data Lifecycle Manager émettent des événements liés aux actions de la politique de cycle de vie. Vous pouvez utiliser AWS Lambda Amazon CloudWatch Events pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur [Amazon](#).

Les événements suivants sont disponibles :

Note

Aucun événement n'est émis pour les actions de politique de cycle de vie des AMI.

- **createSnapshot** : événement Amazon EBS émis en cas de réussite ou d'échec d'une action CreateSnapshot. Pour de plus amples informations, veuillez consulter [EventBridge Événements Amazon pour Amazon EBS](#).
- **DLM Policy State Change** : événement Amazon Data Lifecycle Manager émis lorsqu'une politique de cycle de vie passe en mode erreur. L'événement contient une description de la cause de l'erreur.

Vous trouverez ci-après un exemple d'événement émis lorsque les autorisations accordées par le rôle IAM sont insuffisantes.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "DLM Policy State Change",
  "source": "aws.dlm",
  "account": "123456789012",
  "time": "2018-05-25T13:12:22Z",
  "region": "us-east-1",
```

```

    "resources": [
      "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail": {
      "state": "ERROR",
      "cause": "Role provided does not have sufficient permissions",
      "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
  }
}

```

Voici un exemple d'événement émis lorsqu'une limite est dépassée.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "DLM Policy State Change",
  "source": "aws.dlm",
  "account": "123456789012",
  "time": "2018-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
  ],
  "detail":{
    "state": "ERROR",
    "cause": "Maximum allowed active snapshot limit exceeded",
    "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
  }
}

```

- **DLM Pre Post Script Notification** : événement émis lorsqu'un pré-script ou un post-script est lancé, réussit ou échoue.

Voici un exemple d'événement émis lorsqu'une sauvegarde VSS réussit.

```

{
  "version": "0",
  "id": "12345678-1234-1234-1234-123456789012",
  "detail-type": "DLM Pre Post Script Notification",
  "source": "aws.dlm",
  "account": "123456789012",

```



```

    "time": "2023-10-27T22:04:52Z",
    "region": "us-east-1",
    "resources": ["arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef"],
    "detail": {
      "script_stage": "",
      "result": "success",
      "cause": "",
      "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef",
      "execution_handler": "AWS_VSS_BACKUP",
      "source": "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef",
      "resource_type": "EBS_SNAPSHOT",
      "resources": [{
        "status": "pending",
        "resource_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
        "source": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-01234567890abcdef"
      }],
      "request_id": "a1b2c3d4-a1b2-a1b2-a1b2-a1b2c3d4e5f6",
      "start_time": "2023-10-27T22:03:29.370Z",
      "end_time": "2023-10-27T22:04:51.370Z",
      "timeout_time": ""
    }
  }
}

```

Surveillez les politiques du Data Lifecycle Manager à l'aide de CloudWatch

Vous pouvez surveiller vos politiques de cycle de vie d'Amazon Data Lifecycle Manager à l'aide de CloudWatch, qui collecte les données brutes et les transforme en mesures lisibles en temps quasi réel. Vous pouvez utiliser ces statistiques pour voir exactement combien de snapshots et d'EBS-backed AMI Amazon EBS sont créés, supprimés et copiés par vos politiques au fil du temps. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints.

Les métriques sont enregistrées pour une durée de 15 mois. Vous pouvez, par conséquent, accéder aux informations historiques et mieux comprendre la façon dont vos politiques de cycle de vie s'exécute sur une durée prolongée.

Pour plus d'informations sur Amazon CloudWatch, consultez le guide de CloudWatch l'utilisateur [Amazon](#).

Rubriques

- [Métriques prises en charge](#)
- [Afficher CloudWatch les statistiques relatives à vos politiques](#)
- [Graphique de métriques de vos politiques](#)
- [Créer une CloudWatch alarme pour une politique](#)
- [Exemples de cas d'utilisation](#)
- [Gestion des politiques qui signalent les actions ayant échoué](#)

Métriques prises en charge

Les métriques Amazon Data Lifecycle Manager suivantes sont incluses dans l'AWS/EBS espace de noms. Les indicateurs varient selon le type de politique.

Toutes les métriques peuvent être mesurées dans la dimension `DLMPolicyId`. Les statistiques les plus utiles sont `sum` et `average`, et l'unité de mesure est `count`.

Sélectionnez un onglet pour afficher les métriques prises en charge par le type de politique correspondant.

EBS snapshot policies

Métrique	Description
Resources Targeted	Le nombre de ressources ciblées par les balises spécifiées dans un instantané ou une politique EBS-backed AMI.
Snapshots CreateStarted	<p>Nombre d'actions de création d'instantanés lancées par une politique d'instantané. Chaque action n'est enregistrée qu'une seule fois, même s'il y a plusieurs tentatives ultérieures.</p> <p>Si une action de création d'instantanés échoue, Amazon Data Lifecycle Manager envoie une métrique <code>SnapshotsCreateFailed</code>.</p>
Snapshots CreateCompleted	Nombre d'instantanés créés par une politique d'instantané. Cela inclut les tentatives réussies dans les 60 minutes suivant l'heure prévue.

Métrique	Description
Snapshots CreateFailed	Nombre d'instantanés qui n'ont pas pu être créés par une politique d'instantané. Cela inclut les tentatives infructueuses dans les 60 minutes suivant l'heure prévue.
Snapshots SharedCompleted	Nombre d'instantanés partagés entre les comptes par une politique d'instantané.
Snapshots DeleteCompleted	<p>Le nombre de snapshots supprimés par un snapshot ou une politique EBS-backed AMI. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique.</p> <p>Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique EBS-backed AMI annule l'enregistrement des AMI.</p>
Snapshots DeleteFailed	<p>Le nombre de clichés qui n'ont pas pu être supprimés par un snapshot ou une politique EBS-backed AMI. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique.</p> <p>Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique EBS-backed AMI annule l'enregistrement des AMI.</p>
Snapshots CopiedRegionStarted	Nombre d'actions de copie d'instantanés inter-régions lancées par une politique d'instantané.
Snapshots CopiedRegionCompleted	Nombre de copies d'instantanés inter-régions créées par une politique d'instantané. Cela inclut les tentatives réussies dans les 24 heures suivant l'heure prévue.
Snapshots CopiedRegionFailed	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être créées par une politique d'instantané. Cela inclut les tentatives infructueuses dans les 24 heures suivant l'heure prévue.

Métrique	Description
Snapshots CopiedRegionDeleteCompleted	Nombre de copies d'instantanés inter-régions supprimées, conformément à la règle de rétention, par une politique d'instantané.
Snapshots CopiedRegionDeleteFailed	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être supprimées, conformément à la règle de rétention, par une politique d'instantané.
snapshots ArchiveDeletionFailed	Nombre d'instantanés archivés qui n'ont pas pu être supprimés du niveau d'archivage par une politique d'instantané.
snapshots ArchiveScheduled	Nombre d'instantanés dont l'archivage a été prévu par une politique d'instantané.
snapshots ArchiveCompleted	Nombre d'instantanés qui ont été archivés correctement par une politique d'instantané.
snapshots ArchiveFailed	Nombre d'instantanés qui n'ont pas pu être archivés par une politique d'instantané.
snapshots ArchiveDeletionCompleted	Nombre d'instantanés archivés qui ont été supprimés correctement du niveau d'archivage par une politique d'instantané.
PreScript Started	<p>Nombre d'instances pour lesquelles un pré-script a été lancé avec succès.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>

Métrique	Description
PreScriptCompleted	<p>Nombre d'instances pour lesquelles un pré-script a été terminé avec succès. La métrique est émise même si le pré-script se termine après le délai d'expiration spécifié.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>
PreScriptFailed	<p>Nombre d'instances pour lesquelles un pré-script n'a pas été terminé avec succès. La métrique est émise même si le pré-script se termine après le délai d'expiration spécifié.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>
PostScriptStarted	<p>Nombre d'instances pour lesquelles un post-script a été lancé avec succès.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>
PostScriptCompleted	<p>Nombre d'instances pour lesquelles un post-script a été terminé avec succès. La métrique est émise même si le post-script se termine après le délai d'expiration spécifié.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>
PostScriptFailed	<p>Nombre d'instances pour lesquelles un post-script n'a pas été terminé avec succès. La métrique est émise même si le post-script se termine après le délai d'expiration spécifié.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>

Métrique	Description
VSSBackup Started	<p>Nombre d'instances pour lesquelles une sauvegarde VSS a été lancée avec succès.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>
VSSBackup Completed	<p>Nombre d'instances pour lesquelles une sauvegarde VSS a été terminée avec succès. La métrique est émise même si la sauvegarde VSS se termine après le délai d'expiration spécifié.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>
VSSBackup Failed	<p>Nombre d'instances pour lesquelles une sauvegarde VSS n'a pas été terminée avec succès. La métrique est émise même si la sauvegarde VSS se termine après le délai d'expiration spécifié.</p> <p>Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.</p>

EBS-backed AMI policies

Les mesures suivantes peuvent être utilisées avec les politiques EBS-backed AMI :

Métrique	Description
Resources Targeted	Le nombre de ressources ciblées par les balises spécifiées dans un instantané ou une politique EBS-backed AMI.
Snapshots DeleteCompleted	Le nombre de snapshots supprimés par un snapshot ou une politique EBS-backed AMI. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique.

Métrique	Description
	Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique EBS-backed AMI annule l'enregistrement des AMI.
Snapshots DeleteFailed	<p>Le nombre de clichés qui n'ont pas pu être supprimés par un snapshot ou une politique EBS-backed AMI. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique.</p> <p>Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique EBS-backed AMI annule l'enregistrement des AMI.</p>
Snapshots CopiedRegionDelete Completed	Nombre de copies d'instantanés inter-régions supprimées, conformément à la règle de rétention, par une politique d'instantané.
Snapshots CopiedRegionDelete Failed	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être supprimées, conformément à la règle de rétention, par une politique d'instantané.
ImagesCreateStarted	Le nombre d'CreateImageactions initiées par une politique EBS-backed AMI.
ImagesCreateCompleted	Le nombre d'AMI créées par une politique EBS-backed AMI.
ImagesCreateFailed	Le nombre d'AMI qui n'ont pas pu être créées par une politique d'EBS-backed AMI.

Métrique	Description
ImagesDeregisterCompleted	Le nombre d'AMI annulées par une EBS-backed politique AMI.
ImagesDeregisterFailed	Le nombre d'AMI qui n'ont pas pu être désenregistrées par une EBS-backed politique AMI.
ImagesCopiedRegionStarted	Le nombre d'actions de copie interrégionales initiées par une politique EBS-backed AMI.
ImagesCopiedRegionCompleted	Le nombre de copies d'AMI interrégionales créées par une politique EBS-backed AMI.
ImagesCopiedRegionFailed	Le nombre de copies d'AMI interrégionales qui n'ont pas pu être créées par une politique d'EBS-backed AMI.
ImagesCopiedRegionDeregisterCompleted	Le nombre de copies d'AMI interrégionales annulées, comme indiqué par la règle de conservation, par une politique AMI. EBS-backed
ImagesCopiedRegionDeregisterFailed	Le nombre de copies d'AMI interrégionales qui n'ont pas pu être déenregistrées, comme indiqué par la règle de conservation, par une politique AMI. EBS-backed

Métrique	Description
EnableImageDeprecationCompleted	Le nombre d'AMI qui ont été marquées comme étant obsolètes par une politique d' EBS-backed AMI.
EnableImageDeprecationFailed	Le nombre d'AMI qui n'ont pas pu être marquées comme obsolètes par une politique d'EBS-backed AMI.
EnableCopiedImageDeprecationCompleted	Le nombre de copies d'AMI interrégionales qui ont été marquées comme étant obsolètes par une EBS-backed politique AMI.
EnableCopiedImageDeprecationFailed	Le nombre de copies d'AMI interrégionales qui n'ont pas pu être marquées comme étant obsolètes par une EBS-backed politique AMI.

Cross-account copy event policies

Les métriques suivantes peuvent être utilisées avec les politiques d'événement de copie entre comptes :

Métrique	Description
SnapshotsCopiedAccountStarted	Nombre d'actions de copie d'instantané entre comptes initiées par une politique d'événement de copie entre comptes.

Métrique	Description
Snapshots CopiedAccountCompleted	Nombre d'instantanés copiés à partir d'un autre compte par une politique d'événement de copie entre comptes. Cela inclut les tentatives réussies dans les 24 heures suivant l'heure prévue.
Snapshots CopiedAccountFailed	Nombre d'instantanés qui n'ont pas pu être copiés à partir d'un autre compte par une politique d'événement de copie entre comptes. Cela inclut les tentatives infructueuses dans les 24 heures suivant l'heure prévue.
Snapshots CopiedAccountDeleteCompleted	Nombre de copies d'instantanés inter-régions supprimées, conformément à la règle de rétention, par une politique d'événement de copie entre comptes.
Snapshots CopiedAccountDeleteFailed	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être supprimées, conformément à la règle de rétention, par une politique d'événement de copie entre comptes.

Afficher CloudWatch les statistiques relatives à vos politiques

Vous pouvez utiliser les outils de ligne de commande Console de gestion AWS ou les outils de ligne de commande pour répertorier les mesures qu'Amazon Data Lifecycle Manager envoie à Amazon CloudWatch.

Amazon EC2 console

Pour afficher les métriques à l'aide de la console Amazon EC2

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sélectionnez Lifecycle Manager (Gestionnaire de cycle de vie).
3. Sélectionnez une politique dans la grille, puis sélectionnez l'onglet Monitoring(Surveillance).

CloudWatch console

Pour consulter les statistiques à l'aide de la CloudWatch console Amazon

1. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de nom EBS, puis sélectionnez Data Lifecycle Manager metrics (Métriques Data Lifecycle Manager).

AWS CLI

Pour répertorier toutes les métriques disponibles pour Amazon Data Lifecycle Manager

Utilisez la commande [list-metrics](#).

```
$ C:\> aws cloudwatch list-metrics \  
--namespace AWS/EBS
```

Pour répertorier toutes les métriques d'une politique spécifique

Utilisez la commande [list-metrics](#) et spécifiez la dimension `DLMPolicyId`.

```
$ C:\> aws cloudwatch list-metrics \  
--namespace AWS/EBS \  
--dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

Pour répertorier une métrique unique dans toutes les politiques

Utilisez la commande [list-metrics](#) et spécifiez l'option `--metric-name`.

```
$ C:\> aws cloudwatch list-metrics \  
--namespace AWS/EBS \  
--metric-name SnapshotsCreateCompleted
```

Graphique de métriques de vos politiques

Après avoir créé une politique, vous pouvez ouvrir la console Amazon EC2 et afficher les graphiques de surveillance de la politique dans l'onglet Monitoring (Surveillance). Chaque graphique s'appuie sur l'une des métriques Amazon EC2 disponibles.

Les graphiques de métriques suivants sont disponibles :

- Ressources ciblées (basées sur `ResourcesTargeted`)
- Création d'instantané démarrée (basé sur `SnapshotsCreateStarted`)
- Création d'instantané terminée (basé sur `SnapshotsCreateCompleted`)
- Échec de la création d'instantané (basé sur `SnapshotsCreateFailed`)
- Partage d'instantané terminé (basé sur `SnapshotsSharedCompleted`)
- Suppression d'instantané terminée (basé sur `SnapshotsDeleteCompleted`)
- Échec de la suppression d'instantané (basé sur `SnapshotsDeleteFailed`)
- Copie d'instantané inter-Régions démarrée (basé sur `SnapshotsCopiedRegionStarted`)
- Copie d'instantané inter-Régions terminée (basé sur `SnapshotsCopiedRegionCompleted`)
- Échec de la copie d'instantané inter-Région (basé sur `SnapshotsCopiedRegionFailed`)
- Suppression de copie d'instantané inter-Région terminée (basé sur `SnapshotsCopiedRegionDeleteCompleted`)
- Échec de suppression de copie d'instantané inter-Région (basé sur `SnapshotsCopiedRegionDeleteFailed`)
- Copie d'instantané inter-comptes démarrée (basé sur `SnapshotsCopiedAccountStarted`)
- Copie d'instantané inter-comptes terminée (basé sur `SnapshotsCopiedAccountCompleted`)
- Échec de la copie d'instantané inter-comptes (basé sur `SnapshotsCopiedAccountFailed`)
- Suppressions de copie d'instantané inter-comptes terminées (basé sur `SnapshotsCopiedAccountDeleteCompleted`)
- Échecs de suppression de copie d'instantané inter-comptes (basé sur `SnapshotsCopiedAccountDeleteFailed`)
- Création de l'AMI démarrée (basé sur `ImagesCreateStarted`)
- Créations d'AMI terminées (basé sur `ImagesCreateCompleted`)
- Échec de la création de l'AMI (basé sur `ImagesCreateFailed`)
- Annulations d'enregistrement d'AMI terminées (basé sur `ImagesDeregisterCompleted`)
- Échecs d'annulation d'enregistrement d'AMI (basé sur `ImagesDeregisterFailed`)
- Copie de l'AMI inter-Région commencée (basé sur `ImagesCopiedRegionStarted`)
- Copie de l'AMI inter-Régions terminée (basé sur `ImagesCopiedRegionCompleted`)
- Échec de la copie de l'AMI inter-Régions (basé sur `ImagesCopiedRegionFailed`)

- Annulation de l'enregistrement de la copie inter-Régions de l'AMI terminée (basé sur `ImagesCopiedRegionDeregisterCompleted`)
- Échec de l'annulation de l'enregistrement de la copie inter-Régions AMI (basé sur `ImagesCopiedRegionDeregisteredFailed`)
- Obsolescence de l'option AMI terminée (basé sur `EnableImageDeprecationCompleted`)
- Échec d'activation de l'obsolescence de l'AMI (basé sur `EnableImageDeprecationFailed`)
- Copie de l'AMI inter-Régions pour activer l'obsolescence terminée (basé sur `EnableCopiedImageDeprecationCompleted`)
- Échec de l'activation de l'obsolescence de la copie inter-région AMI (basé sur `EnableCopiedImageDeprecationFailed`)

Créer une CloudWatch alarme pour une politique

Vous pouvez créer une CloudWatch alarme qui surveille CloudWatch les indicateurs de vos politiques. CloudWatch vous enverra automatiquement une notification lorsque la métrique atteint un seuil que vous avez spécifié. Vous pouvez créer une CloudWatch alarme à l'aide de la CloudWatch console.

Pour plus d'informations sur la création d'alarmes à l'aide de la CloudWatch console, consultez la rubrique suivante du Guide de CloudWatch l'utilisateur Amazon.

- [Création d'une CloudWatch alarme basée sur un seuil statique](#)
- [Création d'une CloudWatch alarme basée sur la détection d'anomalies](#)

Exemples de cas d'utilisation

Voici des exemples de cas d'utilisation :

Rubriques

- [Exemple 1 : ResourcesTargeted métrique](#)
- [Exemple 2 : SnapshotDeleteFailed métrique](#)
- [Exemple 3 : SnapshotsCopiedRegionFailed métrique](#)

Exemple 1 : ResourcesTargeted métrique

Vous pouvez utiliser la métrique `ResourcesTargeted` pour surveiller le nombre total de ressources ciblées par une politique spécifique chaque fois qu'elle est exécutée. Cela vous permet de déclencher une alarme lorsque le nombre de ressources ciblées est inférieur ou supérieur à un seuil attendu.

Par exemple, si vous attendez à ce que votre politique quotidienne crée des sauvegardes ne dépassant pas 50 volumes, vous pouvez créer une alarme qui envoie une notification par e-mail lorsque la somme pour `ResourcesTargeted` est supérieure à 50 sur une période de 1 heure. Vous pouvez ainsi vous assurer qu'aucun instantané n'a été créé de manière inattendue à partir de volumes mal balisés.

Vous pouvez utiliser la commande suivante pour créer cette alarme :

```
$ C:\> aws cloudwatch put-metric-alarm \  
  --alarm-name resource-targeted-monitor \  
  --alarm-description "Alarm when policy targets more than 50 resources" \  
  --metric-name ResourcesTargeted \  
  --namespace AWS/EBS \  
  --statistic Sum \  
  --period 3600 \  
  --threshold 50 \  
  --comparison-operator GreaterThanThreshold \  
  --dimensions "Name=DLMPolicyId,Value=policy_id" \  
  --evaluation-periods 1 \  
  --alarm-actions sns_topic_arn
```

Exemple 2 : SnapshotDeleteFailed métrique

Vous pouvez utiliser la métrique `SnapshotDeleteFailed` pour surveiller les échecs de suppression des instantanés conformément à la règle de rétention des instantanés de la politique.

Par exemple, si vous avez créé une politique qui doit supprimer automatiquement les instantanés toutes les douze heures, vous pouvez créer une alarme qui avertit votre équipe d'ingénierie lorsque la somme pour `SnapshotDeletionFailed` est supérieure à 0 sur une période de 1 heure. Cela peut vous aider à identifier une mauvaise conservation des instantanés et à vous assurer que vos coûts de stockage ne sont pas augmentés par des instantanés inutiles.

Vous pouvez utiliser la commande suivante pour créer cette alarme :

```
$ C:\> aws cloudwatch put-metric-alarm \  
  --alarm-name snapshot-deletion-failed-monitor \  
  --alarm-description "Alarm when snapshot deletions fail" \  
  --metric-name SnapshotsDeleteFailed \  
  --namespace AWS/EBS \  
  --statistic Sum \  
  --period 3600 \  
  --threshold 0 \  
  --comparison-operator GreaterThanThreshold \  
  --dimensions "Name=DLMPolicyId,Value=policy_id" \  
  --evaluation-periods 1 \  
  --alarm-actions sns_topic_arn
```

Exemple 3 : SnapshotsCopiedRegionFailed métrique

Utilisez la métrique `SnapshotsCopiedRegionFailed` pour identifier lorsque vos politiques ne parviennent pas à copier des instantanés vers d'autres régions.

Par exemple, si votre politique copie quotidiennement des instantanés entre régions, vous pouvez créer une alarme qui envoie un SMS à votre équipe d'ingénierie lorsque la somme pour `SnapshotCrossRegionCopyFailed` est supérieure à 0 sur une période de 1 heure. Cela peut être utile pour vérifier si les instantanés suivants de la lignée ont été copiés avec succès par la politique.

Vous pouvez utiliser la commande suivante pour créer cette alarme :

```
$ C:\> aws cloudwatch put-metric-alarm \  
  --alarm-name snapshot-copy-region-failed-monitor \  
  --alarm-description "Alarm when snapshot copy fails" \  
  --metric-name SnapshotsCopiedRegionFailed \  
  --namespace AWS/EBS \  
  --statistic Sum \  
  --period 3600 \  
  --threshold 0 \  
  --comparison-operator GreaterThanThreshold \  
  --dimensions "Name=DLMPolicyId,Value=policy_id" \  
  --evaluation-periods 1 \  
  --alarm-actions sns_topic_arn
```

Gestion des politiques qui signalent les actions ayant échoué

Pour plus d'informations sur la marche à suivre lorsque l'une de vos politiques indique une valeur inattendue différente de zéro pour une mesure d'action ayant échoué, consultez l'article [Que dois-](#)

[je faire si Amazon Data Lifecycle Manager signale des actions ayant échoué dans les CloudWatch métriques ?](#)

Journalisation des appels d'API Amazon Data Lifecycle Manager avec AWS CloudTrail

Avec AWS CloudTrail, vous pouvez suivre l'activité des utilisateurs et l'utilisation des API pour démontrer la conformité aux politiques internes et aux normes réglementaires. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS CloudTrail](#).

Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon Data Lifecycle Manager. CloudTrail capture tous les appels d'API pour Amazon Data Lifecycle Manager sous forme d'événements, y compris les appels depuis la console Amazon Data Lifecycle Manager et les appels de code vers les API Amazon Data Lifecycle Manager. Si vous créez un historique, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon Data Lifecycle Manager. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents sur la CloudTrail console dans l'historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Amazon Data Lifecycle Manager, l'adresse IP à partir de laquelle la demande a été faite, qui l'a faite, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le Guide de [AWS CloudTrail l'utilisateur](#).

Informations sur Amazon Data Lifecycle Manager dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Amazon Data Lifecycle Manager, elle est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents sur votre AWS compte. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#).

Pour un enregistrement permanent des événements de votre AWS compte, y compris les événements relatifs à Amazon Data Lifecycle Manager, créez un historique. Un journal permet CloudTrail de transmettre des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS

services pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux et y donner suite. Pour en savoir plus, consultez :

- [Présentation de la création d'un journal d'activité](#)
- [CloudTrail Services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux provenant de plusieurs régions](#) et [réception de fichiers CloudTrail journaux provenant de plusieurs comptes](#)

Toutes les actions d'Amazon Data Lifecycle Manager sont enregistrées par CloudTrail. Par exemple, les appels aux DeleteLifecyclePolicy actions CreateLifecyclePolicy et génèrent des entrées dans les fichiers CloudTrail journaux. Pour la liste complète des actions, voir [Actions](#).

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 les éléments suivants :

- Quel utilisateur a fait la demande.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez la section [Élément userIdentity CloudTrail](#).

Comprendre les entrées des fichiers journaux d'Amazon Data Lifecycle Manager

Un journal est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une pile ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Exemple Exemple : CreateLifecyclePolicy

Voici un exemple d'entrée de CloudTrail journal pour cette CreateLifecyclePolicy action.

```
{
```

```

"eventVersion": "1.05",
"userIdentity": {
  "type": "Root",
  "principalId": "123456789012",
  "arn": "arn:aws:iam::123456789012:root",
  "accountId": "123456789012",
  "accessKeyId": "AKIAJA2ELRVCPEXAMPLE",
  "userName": "user",
  "sessionContext": {
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2018-07-24T18:01:05Z"
    }
  }
},
"eventTime": "2018-07-24T18:20:28Z",
"eventSource": "dlm.amazonaws.com",
"eventName": "CreateLifecyclePolicy",
"awsRegion": "us-west-2",
"sourceIPAddress": "54.240.230.179",
"userAgent": "console.ec2.amazonaws.com",
"requestParameters": {
  "ExecutionRoleArn": "arn:aws:iam::123456789012:role/service-role/
AWSDataLifecycleManagerServiceRole",
  "PolicyDetails": {
    "ResourceTypes": [
      "VOLUME"
    ],
    "Schedules": [
      {
        "CreateRule": {
          "Interval": 12,
          "IntervalUnit": "HOURS",
          "Times": [
            "09:00"
          ]
        },
        "Name": "Default Schedule",
        "RetainRule": {
          "Count": 3
        },
        "TagsToAdd": [
          {
            "Key": "Name",

```

```

        "Value": "backup-my-volume"
      }
    ]
  },
  "TargetTags": [
    {
      "Key": "Name",
      "Value": "my-volume"
    }
  ]
},
"Description": "test-cloudtrail",
"State": "DISABLED"
},
"responseElements": {
  "PolicyId": "policy-04ff8755fce0599eb"
},
"requestID": "3d714ca6-8f6e-11e8-92a4-35fd765427f0",
"eventID": "28ab3121-6040-4a40-80c7-ae59b3adf405",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}

```

Exemple Exemple : DeleteLifecyclePolicy

Voici un exemple d'entrée de CloudTrail journal pour cette DeleteLifecyclePolicy action.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAJA2ELRVCPEXAMPLE",
    "userName": "user",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-07-24T18:01:05Z"
      }
    }
  }
}

```

```
  },
  "eventTime": "2018-07-24T19:33:33Z",
  "eventSource": "dlm.amazonaws.com",
  "eventName": "DeleteLifecyclePolicy",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "54.240.230.241",
  "userAgent": "console.ec2.amazonaws.com",
  "requestParameters": {
    "policyId": "policy-04ff8755fce0599eb"
  },
  "responseElements": null,
  "requestID": "73260971-8f78-11e8-a156-598016e53fb2",
  "eventID": "3740f2fb-0d6a-4712-a7ad-eb9f17103fb2",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Points de terminaison de service pour Amazon Data Lifecycle Manager

Un point de terminaison est une URL qui sert de point d'entrée à un service AWS Web. Amazon Data Lifecycle Manager prend en charge les types de terminaux suivants :

- Points de terminaison IPv4
- Dual-stack terminaux prenant en charge à la fois IPv4 et IPv6
- Points de terminaison FIPS

Lorsque vous faites une demande, vous pouvez spécifier le point de terminaison et la région à utiliser. Si vous ne spécifiez pas de point de terminaison, le point de terminaison IPv4 est utilisé par défaut. Pour utiliser un autre type de point de terminaison, vous devez le spécifier dans votre demande. Pour obtenir un exemple de la façon de procéder, consultez [Spécification des points de terminaison](#).

Pour Amazon Data Lifecycle Manager, voir les points de terminaison [Amazon Data Lifecycle Manager](#) dans le Référence générale d'Amazon Web Services.

Rubriques

- [Points de terminaison IPv4](#)

- [Dual-stack terminaux \(IPv4 et IPv6\)](#)
- [Points de terminaison FIPS](#)
- [Spécification des points de terminaison](#)

Points de terminaison IPv4

Les points de terminaison IPv4 prennent en charge le trafic IPv4 uniquement. Les points de terminaison IPv4 sont disponibles pour toutes les régions.

Vous devez spécifier la région dans le nom du point de terminaison. Les noms des points de terminaison utilisent la convention de dénomination suivante :

- `d1m.region.amazonaws.com`

Par exemple, le point de terminaison IPv4 pour la région USA Est (Virginie du Nord) est `d1m.us-east-1.amazonaws.com`.

Dual-stack terminaux (IPv4 et IPv6)

Dual-stack les terminaux prennent en charge le trafic IPv4 et IPv6. Dual-stack les points de terminaison sont disponibles pour toutes les régions.

Pour utiliser IPv6, vous devez utiliser un point de terminaison à double pile. Lorsque vous adressez une requête à un point de terminaison à double pile, l'URL du point de terminaison se résout en une adresse IPv6 ou IPv4, selon le protocole utilisé par votre réseau et votre client.

Vous devez spécifier la région dans le nom du point de terminaison. Dual-stack les noms de points de terminaison utilisent la convention de dénomination suivante :

- `d1m.region.api.aws`

Par exemple, le point de terminaison à double pile pour la région de l'Est des États-Unis (Virginie du Nord) est `d1m.us-east-1.api.aws`.

Points de terminaison FIPS

Amazon Data Lifecycle Manager fournit des points de terminaison FIPS-validated à double pile (IPv4 et IPv6) pour les régions suivantes :

- `us-east-1` : USA Est (Virginie du Nord)
- `us-east-2` : USA Est (Ohio)
- `us-west-1` : USA Ouest (Californie du Nord)
- `us-west-2` : USA Ouest (Oregon)
- `ca-central-1` : Canada (Centre)
- `ca-west-1` — Canada-Ouest (Calgary)

Les points de terminaison FIPS à double pile utilisent la convention de dénomination suivante : `d1m-fips.region.api.aws`. Par exemple, le point de terminaison FIPS à double pile pour la région de l'Est des États-Unis (Virginie du Nord) est `d1m-fips.us-east-1.api.aws`.

Spécification des points de terminaison

Les exemples suivants montrent comment spécifier un point de terminaison pour la région US East (N. Virginia) à l'aide de AWS CLI.

- Dual-stack

```
aws dlm create-default-role \  
--resource-type snapshot \  
--endpoint-url https://d1m.us-east-2.api.aws
```

- IPv4

```
aws dlm create-default-role \  
--resource-type snapshot \  
--endpoint-url https://d1m.us-east-2.amazonaws.com
```

Création d'une connexion privée entre un VPC et Amazon EBS

Vous pouvez établir une connexion privée entre votre VPC et Amazon EBS en créant une interface VPC endpoint, alimentée par [AWS PrivateLink](#). Vous pouvez accéder à Amazon EBS comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérie NAT, de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec Amazon EBS.

Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface.

Pour plus d'informations, consultez la section [Accès Services AWS via AWS PrivateLink](#) le AWS PrivateLink Guide.

 Note

Amazon Data Lifecycle Manager prend en charge les points de terminaison VPC à interface IPv4 pour toutes les zones commerciales et les AWS GovCloud (US) régions, et les points de terminaison VPC à interface IPv6 pour les régions commerciales uniquement.

Considérations relatives aux points de terminaison Amazon EBS VPC

Avant de configurer un point de terminaison VPC d'interface pour Amazon EBS, consultez les [considérations du](#) AWS PrivateLink Guide.

Par défaut, l'accès complet à Amazon EBS est autorisé via le point de terminaison. Vous pouvez contrôler l'accès au point de terminaison de l'interface à l'aide des politiques de point de terminaison VPC. Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès à Amazon EBS. La politique spécifie les informations suivantes :

- Le `principal` qui peut effectuer des actions.
- Les `actions` qui peuvent être effectuées.
- Les `ressources` sur lesquelles les actions peuvent être effectuées.

Pour de plus amples informations, veuillez consulter [Contrôle de l'accès aux services avec points de terminaison d'un VPC](#) dans le Amazon VPC Guide de l'utilisateur.

Voici un exemple de politique relative aux terminaux pour Amazon EBS. Lorsqu'elle est associée à un point de terminaison, cette politique autorise tous les utilisateurs à obtenir des informations récapitulatives sur les politiques d'Amazon Data Lifecycle Manager.

```
{
  "Statement": [{
    "Action": "dlm:GetLifecyclePolicies",
    "Effect": "Allow",
    "Principal": "*",
```

```
"Resource": "*"
}]
}
```

Création d'un point de terminaison VPC d'interface pour Amazon EBS

Vous pouvez créer un point de terminaison VPC pour Amazon EBS à l'aide de la console Amazon VPC ou du AWS Command Line Interface (CLI). Pour plus d'informations, consultez [Créer un point de terminaison d'un VPC](#) dans le Guide AWS PrivateLink .

Créez un point de terminaison VPC pour Amazon EBS en utilisant le nom de service suivant :

- `com.amazonaws.region.dlm`

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à Amazon EBS en utilisant son nom DNS par défaut pour la région, `dlm.us-east-1.amazonaws.com` par exemple.

Résoudre les problèmes liés à Amazon Data Lifecycle Manager

La documentation suivante peut vous aider à résoudre les problèmes que vous pouvez rencontrer.

Rubriques

- [Erreur : le rôle dont le nom existe déjà](#)

Erreur : le rôle dont le nom existe déjà

Description

Vous recevez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists` ou `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` lorsque vous essayez de créer une politique à l'aide de la console.

Cause

Le format ARN du rôle par défaut diffère selon qu'il a été créé à l'aide de la console ou de l'AWS CLI. Bien que les ARN soient différents, les rôles utilisent le même nom de rôle, ce qui entraîne un conflit de dénomination des rôles entre la console et l'AWS CLI.

Solution

Pour résoudre ce problème, procédez comme suit :

1. (Pour les politiques de capture instantanée activées pour les pré-scripts et les post-scripts uniquement) Attachez manuellement la politique `AWSDatalifecycleManagerSSMFullAccess` AWS gérée au rôle `AWSDatalifecycleManagerDefaultRole` IAM. Pour plus d'informations, consultez [Ajout des autorisations d'identité IAM](#).
2. Lorsque vous créez votre politique Amazon Data Lifecycle Manager, pour le rôle IAM, sélectionnez Choisir un autre rôle, puis sélectionnez soit `AWSDatalifecycleManagerDefaultRole` (pour une politique de snapshot), soit `AWSDatalifecycleManagerDefaultRoleForAMIManagement` (pour une politique AMI).
3. Continuez à créer la politique comme d'habitude.

AWS Backup pour Amazon Elastic Block Store

AWS Backup est un service entièrement géré qui centralise et automatise la protection des données dans l'ensemble AWS de votre environnement. Plutôt que de gérer les calendriers des snapshots et leur conservation par ressource, vous définissez une politique de sauvegarde unique et vous l'appliquez à l'ensemble des comptes et des régions. Marquez vos ressources et AWS Backup protègez-les automatiquement, sans qu'aucune configuration par équipe ne soit requise. Le service prend en charge de nombreux AWS services, notamment Amazon EBS, Amazon EC2, Amazon S3, Amazon EFS, Amazon RDS et Aurora. Par conséquent, une seule politique peut protéger les volumes, les bases de données, les systèmes de fichiers et les magasins d'objets ensemble sans outils de sauvegarde distincts par charge de travail.

Pour Amazon EBS, AWS Backup fournit des instantanés multivolumes cohérents en cas de panne qui coordonnent les sauvegardes ponctuelles sur tous les volumes attachés à une instance Amazon EC2. Cela est essentiel pour les bases de données et les applications en cluster qui couvrent plusieurs volumes. AWS Backup La fonction de recherche va encore plus loin en permettant la restauration au niveau de l'élément. Vous pouvez localiser et restaurer des fichiers ou des répertoires individuels à partir d'instantanés Amazon EBS sans restaurer l'intégralité du volume.

AWS Backup ajoute également une sécurité et une conformité de niveau professionnel à vos instantanés. Les coffres-forts ventilés isolent logiquement les points de restauration de votre environnement de production. Vault Lock impose l'immuabilité. GuardDuty L'intégration Amazon analyse les sauvegardes à la recherche de logiciels malveillants. Backup Audit Manager évalue en permanence votre posture de sauvegarde et génère des rapports de conformité prêts à être audités.

Pour commencer, consultez les ressources suivantes :

- [AWS Backup Manuel du développeur](#)
- [Créez des sauvegardes multivolumes cohérentes en cas de crash](#)
- [Restaurer les volumes Amazon EBS](#)
- [Recherchez et récupérez des fichiers individuels à partir d'instantanés Amazon EBS](#)

Utiliser API directes EBS pour accéder au contenu d'un instantané EBS

Vous pouvez utiliser les API Amazon Elastic Block Store (Amazon EBS) directes pour créer des instantanés EBS, écrire des données directement sur vos instantanés, lire des données sur vos instantanés et identifier les différences ou les modifications entre deux instantanés. Si vous êtes un fournisseur indépendant de logiciel (FIL) qui offre des services de sauvegarde pour Amazon EBS, il est plus rentable et efficace d'utiliser les API directes EBS pour de suivre les modifications incrémentielles sur vos volumes EBS via des instantanés EBS à l'aide des instantanés. Pour ce faire, vous n'avez pas besoin de créer des volumes à partir d'instantanés, puis d'utiliser des instances Amazon Elastic Compute Cloud (Amazon EC2) pour comparer leurs différences.

Vous pouvez créer des instantanés incrémentiels directement à partir de données locales dans des volumes EBS et dans le cloud afin de les utiliser pour une reprise après sinistre rapide. Avec la possibilité d'écrire et de lire des instantanés, vous pouvez écrire vos données locales dans un instantané EBS lors d'un sinistre. Après la restauration, vous pouvez ensuite le restaurer sur site AWS ou sur site à partir de l'instantané. Vous n'avez plus besoin de créer et de gérer des mécanismes complexes pour copier des données depuis et vers Amazon EBS.

Le présent guide de l'utilisateur fournit une vue d'ensemble des éléments qui composent les API directes EBS, ainsi que des exemples d'utilisation efficace de ces éléments. Pour plus d'informations sur les actions, les types de données, les paramètres et les erreurs des API, consultez la [référence des API directes EBS](#). Pour plus d'informations sur les AWS régions, les points de terminaison et les quotas de service pris en charge pour les API directes EBS, consultez la section Points de terminaison et quotas [Amazon EBS dans le](#). Références générales AWS

Rubriques

- [Tarification des API directes EBS](#)
- [Concepts pour les API EBS Direct](#)
- [Contrôlez l'accès aux API EBS Direct à l'aide d'IAM](#)
- [Lisez les instantanés Amazon EBS avec les API EBS Direct](#)
- [Rédigez des instantanés Amazon EBS avec les API EBS Direct](#)
- [Résultats du chiffrement pour les API EBS Direct](#)
- [Utilisez les sommes de contrôle des API directes EBS pour valider les données des instantanés](#)

- [Garantir l'idempotence dans StartSnapshot les requêtes d'API](#)
- [Rétentatives d'erreur pour les API EBS Direct](#)
- [Optimisez les performances des API EBS Direct](#)
- [Points de terminaison de service pour les API EBS Direct](#)
- [AWS Exemples de code SDK pour les API EBS Direct](#)
- [Création d'une connexion privée entre un VPC et les API directes EBS](#)
- [Enregistrez les appels d'API directs EBS à l'aide de AWS CloudTrail](#)
- [Questions fréquemment posées sur les API EBS Direct](#)

Tarification des API directes EBS

Tarification des API

Le prix que vous payez pour utiliser le API directes EBS dépend des demandes que vous faites. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

- ListChangedBlockset ListSnapshotBlocks les API sont facturées par demande. Par exemple, si vous effectuez 100 000 demandes d' ListSnapshotBlocks API dans une région facturant 0,0006 USD pour 1 000 demandes, vous serez facturé 0,06 USD (0,0006 USD pour 1 000 demandes x 100).
- GetSnapshotBlockest facturé par bloc retourné. Par exemple, si vous effectuez 100 000 demandes d' GetSnapshotBlock API dans une région facturant 0,003 USD pour 1 000 blocs renvoyés, vous serez facturé 0,30 USD (0,003 USD pour 1 000 blocs renvoyés x 100).
- PutSnapshotBlockest facturé par bloc écrit. Par exemple, si vous effectuez 100 000 demandes d' PutSnapshotBlock API dans une région facturant 0,006\$ pour 1 000 blocs écrits, vous serez facturé 0,60\$ (0,006\$ pour 1 000 blocs écrits x 100).

Coûts de mise en réseau

Coûts de transfert des données

Les données transférées directement entre les API EBS Direct et les instances Amazon EC2 dans la même AWS région sont gratuites lorsque vous utilisez des points de terminaison [non FIPS](#). Pour plus d'informations, consultez [Points de terminaison du service AWS](#). Si d'autres AWS services font

obstacle à votre transfert de données, les frais de traitement des données associés vous seront facturés. Ces services incluent, sans toutefois s'y limiter, les PrivateLink points de terminaison, la passerelle NAT et la passerelle de transit.

Points de terminaison de l'interface d'un VPC

Si vous utilisez des API EBS directes provenant d'instances ou de AWS Lambda fonctions Amazon EC2 dans des sous-réseaux privés, vous pouvez utiliser des points de terminaison d'interface VPC, au lieu d'utiliser des passerelles NAT, afin de réduire les coûts de transfert de données réseau. Pour de plus amples informations, veuillez consulter [Création d'une connexion privée entre un VPC et les API directes EBS](#).

Concepts pour les API EBS Direct

Voici les concepts clés que vous devez comprendre avant de commencer à utiliser les API EBS Direct.

Instantanés

Les instantanés représentent le principal moyen de sauvegarde des données de vos volumes EBS. Avec le API directes EBS, vous pouvez également sauvegarder des données de vos disques locaux vers des instantanés. Afin d'économiser les frais de stockage, les instantanés successifs sont incrémentiels ; ils contiennent uniquement les données du volume ayant changé depuis l'instantané précédent. Pour de plus amples informations, veuillez consulter [Instantanés Amazon EBS](#).

Note

Les API EBS direct ne prennent pas en charge les instantanés publics et les instantanés locaux sur AWS Outposts

Blocs

Un bloc est un fragment de données au sein d'un instantané. Chaque instantané peut contenir des milliers de blocs. Tous les blocs d'un instantané sont de taille fixe.

Index de bloc

Un index de blocs est un index logique en unités de 512 blocs Kio. Pour identifier l'index de blocs, divisez le décalage logique des données dans le volume logique par la taille de bloc (décalage logique des données/524288). Le décalage logique des données doit être 512 aligné en Kio.

Jetons de bloc

Un jeton de bloc est le hachage d'identification d'un bloc dans un instantané. Il est utilisé pour localiser les données de bloc. Les jetons de bloc renvoyés par les API directes EBS sont temporaires. Ils changent selon l'horodatage d'expiration qui leur est spécifié, ou si vous en exécutez un autre `ListSnapshotBlocks` ou `ListChangedBlocks` demandez le même instantané.

Total de contrôle

Une somme de contrôle est une référence de petite taille dérivée d'un bloc de données dans le but de détecter les erreurs introduites lors de sa transmission ou de son stockage. Les API directes EBS utilisent les sommes de contrôle pour valider l'intégrité des données. Lorsque vous lisez les données d'un instantané EBS, le service fournit des sommes de contrôle Base64-encodées SHA256 pour chaque bloc de données transmis, que vous pouvez utiliser à des fins de validation. Lorsque vous écrivez des données dans un instantané EBS, vous devez fournir une somme de contrôle SHA256 codée en Base64 pour chaque bloc de données transmis. Le service valide les données reçues à l'aide de la somme de contrôle fournie. Pour plus d'informations, consultez [Utilisez les sommes de contrôle des API directes EBS pour valider les données des instantanés](#) plus loin dans ce guide.

Chiffrement

Le chiffrement protège vos données en les convertissant en code illisible qui ne peut être déchiffré que par les personnes ayant accès à la clé KMS utilisée pour les chiffrer. Vous pouvez utiliser les API directes EBS pour lire et écrire des instantanés chiffrés, mais il existe certaines limitations. Pour plus d'informations, consultez [Résultats du chiffrement pour les API EBS Direct](#) plus loin dans ce guide.

Actions d'API

Les API directes EBS se composent de six actions. Il y a trois actions de lecture et trois actions d'écriture. Les actions de lecture sont :

- `ListSnapshotBlocks`— renvoie les index de blocs et les jetons de bloc des blocs dans l'instantané spécifié

- **ListChangedBlocks**— renvoie les index de bloc et les jetons de bloc des blocs qui sont différents entre deux instantanés spécifiés du même volume et de la même lignée d'instantanés.
- **GetSnapshotBlock**— renvoie les données dans un bloc pour l'ID de snapshot, l'index de bloc et le jeton de bloc spécifiés.

Les actions d'écriture sont :

- **StartSnapshot**— lance un instantané, soit en tant qu'instantané incrémentiel d'un instantané existant, soit en tant que nouveau cliché. L'instantané démarré reste en attente jusqu'à ce qu'il soit terminé à l'aide de l' **CompleteSnapshot** action.
- **PutSnapshotBlock**— ajoute des données à un instantané démarré sous la forme de blocs individuels. Vous devez spécifier une somme de contrôle Base64-encoded SHA256 pour le bloc de données transmis. Le service valide le total de contrôle après la fin de la transmission des données. La requête échoue lorsque le total de contrôle calculé par le service ne correspond pas à la valeur que vous avez spécifiée.
- **CompleteSnapshot**— complète une capture d'écran démarrée qui est en attente. L'instantané passe alors à l'état terminé.

Signature Version 4 (signature)

Signature Version 4 est le processus permettant d'ajouter des informations d'authentification aux AWS demandes envoyées par HTTP. Pour des raisons de sécurité, la plupart des demandes AWS doivent être signées à l'aide d'une clé d'accès, qui consiste en un identifiant de clé d'accès et une clé d'accès secrète. Ces deux clés sont généralement appelées informations d'identification de sécurité. Pour plus d'informations sur la façon d'obtenir les informations d'identification permettant d'accéder à votre compte, reportez-vous à [Informations d'identification de sécurité AWS](#).

Si vous avez l'intention de créer manuellement des requêtes HTTP, vous devez apprendre à les signer. Lorsque vous utilisez le AWS Command Line Interface (AWS CLI) ou l'un des AWS kits SDK pour envoyer des demandes AWS, ces outils signent automatiquement les demandes pour vous à l'aide de la clé d'accès que vous avez spécifiée lors de la configuration des outils. Lorsque vous utilisez ces derniers, vous n'avez pas besoin d'apprendre à signer vous-même les demandes.

Pour plus d'informations, consultez la section [Signer des demandes d' AWS API](#) dans le guide de l'utilisateur IAM.

Contrôlez l'accès aux API EBS Direct à l'aide d'IAM

Un utilisateur doit disposer des politiques suivantes pour pouvoir utiliser les API directes EBS. Pour plus d'informations, consultez [Modification des autorisations d'un utilisateur](#).

Pour plus d'informations sur les ressources, les actions et les clés de contexte de condition des API directes EBS à utiliser dans les stratégies d'autorisation IAM, consultez [Actions, ressources et clés de condition pour Amazon Elastic Block Store](#) dans la Référence de l'autorisation de service.

Important

Soyez prudent lorsque vous affectez les stratégies suivantes aux utilisateurs . En attribuant ces politiques, vous pouvez donner accès à un utilisateur qui se voit refuser l'accès à la même ressource via les API Amazon EC2, telles que les actions CopySnapshot ou CreateVolume .

Autorisations de lire des instantanés

La politique suivante permet d'utiliser les API EBS direct de lecture sur tous les instantanés d'une région spécifique AWS . Dans la politique, remplacez *<Region>* par la région de l'instantané.

La stratégie suivante permet d'utiliser la lecture API directes EBS sur les instantanés avec une balise clé-valeur spécifique. Dans la politique, remplacez *<Key>* par la valeur clé de la balise et *<Value>* par la valeur de la balise.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
```



```

        "Condition": {
            "StringEqualsIgnoreCase": {
                "aws:ResourceTag/<Key>": "<Value>"
            }
        }
    }
}

```

La stratégie suivante permet d'utiliser toutes les API directes EBS de lecture sur tous les instantanés du compte uniquement dans une plage de temps spécifique. Cette stratégie autorise l'utilisation du API directes EBS basé sur la clé de condition `aws:CurrentTime` globale. Dans la politique, veuillez à remplacer la plage de dates et d'heures affichée par la plage de dates et d'heures de votre politique.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}

```

Pour plus d'informations, consultez [Modification des autorisations d'un utilisateur](#) dans le Guide de l'utilisateur IAM.

Autorisations d'écrire des instantanés

La politique suivante permet d'utiliser les API d'écriture directe EBS sur tous les instantanés d'une région spécifique AWS . Dans la politique, remplacez *<Region>* par la région de l'instantané.

La stratégie suivante permet d'utiliser les API directes EBS d'écriture sur les instantanés avec une balise clé-valeur spécifique. Dans la politique, remplacez *<Key>* par la valeur clé de la balise et *<Value>* par la valeur de la balise.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock",
        "ebs:CompleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "aws:ResourceTag/<Key>": "<Value>"
        }
      }
    }
  ]
}
```

La politique suivante permet l'utilisation de toutes les API directes EBS. Elle n'autorise également l'action StartSnapshot que si un ID d'instantané parent est spécifié. Par conséquent, cette politique bloque la possibilité de démarrer de nouveaux instantanés sans utiliser un instantané parent.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ebs:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
        }
      }
    }
  ]
}
```

La politique suivante permet l'utilisation de toutes les API directes EBS. Il permet également de créer uniquement la clé de balise `user` pour un nouvel instantané. Cette politique garantit également que l'utilisateur dispose de l'accès approprié pour créer des balises. L'action `StartSnapshot` est la seule action qui peut spécifier des balises.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ebs:*",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "user"
        }
      }
    },
    {
      "Effect": "Allow",
```

```

        "Action": "ec2:CreateTags",
        "Resource": "*"
    }
]
}

```

La stratégie suivante permet d'utiliser toutes les API directes EBS d'écriture sur tous les instantanés du compte uniquement dans une plage de temps spécifique. Cette stratégie autorise l'utilisation du API directes EBS basé sur la clé de condition `aws:CurrentTime` globale. Dans la politique, veuillez à remplacer la plage de dates et d'heures affichée par la plage de dates et d'heures de votre politique.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock",
        "ebs:CompleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:*::snapshot/*",
      "Condition": {
        "DateGreaterThan": {
          "aws:CurrentTime": "2018-05-29T00:00:00Z"
        },
        "DateLessThan": {
          "aws:CurrentTime": "2020-05-29T23:59:59Z"
        }
      }
    }
  ]
}

```

Pour plus d'informations, consultez [Modification des autorisations d'un utilisateur](#) dans le Guide de l'utilisateur IAM.

Autorisations d'utilisation AWS KMS keys

La politique suivante accorde les autorisations permettant de déchiffrer un instantané chiffré à l'aide d'une clé KMS spécifique. Elle permet également de chiffrer de nouveaux instantanés à l'aide de la clé KMS par défaut pour le chiffrement EBS. Dans la politique, remplacez *<Region>* par la région de la clé KMS, *<AccountId>* par l'ID du AWS compte de la clé KMS et *<KeyId>* par l'ID de la clé KMS.

Note

Par défaut, tous les administrateurs du compte ont accès à la clé KMS AWS gérée par défaut pour le chiffrement Amazon EBS, et ils peuvent l'utiliser pour les opérations de chiffrement et de déchiffrement EBS. Si vous utilisez une clé gérée par le client, vous devez créer une nouvelle politique de clé ou modifier la politique de clé existante pour la clé gérée par le client afin d'accorder au principal l'accès à la clé gérée par le client. Pour plus d'informations, consultez [Politiques de clé dans AWS KMS](#) dans le Guide du développeur AWS Key Management Service .

Tip

Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour permettre à l'utilisateur de créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée pour le compte de l'utilisateur par un AWS service, comme illustré dans l'exemple suivant.

Pour plus d'informations, consultez [Modification des autorisations d'un utilisateur](#) dans le Guide de l'utilisateur IAM.

Lisez les instantanés Amazon EBS avec les API EBS Direct

Les étapes suivantes décrivent comment utiliser les API directes EBS pour lire des instantanés:

1. Utilisez cette `ListSnapshotBlocks` action pour afficher tous les index de blocs et les jetons de bloc des blocs dans un instantané. Vous pouvez également utiliser cette `ListChangedBlocks` action pour afficher uniquement les index de blocs et les jetons de bloc des blocs qui sont différents entre deux instantanés du même volume et de la même lignée d'instantanés. Ces actions vous aident à

identifier les jetons de bloc et les index de bloc des blocs pour lesquels vous pouvez obtenir des données.

2. Utilisez l' `GetSnapshotBlock` action et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données.

Note

Vous ne pouvez pas utiliser les API EBS Direct avec des instantanés archivés.

Les exemples suivants montrent comment lire des instantanés à l'aide des API directes EBS.

Rubriques

- [Liste des blocs dans un instantané](#)
- [Liste des blocs qui sont différents entre deux instantanés](#)
- [Obtenir des données de bloc à partir d'un instantané](#)

Liste des blocs dans un instantané

AWS CLI

L'exemple de commande [list-snapshot-blocks](#) suivant renvoie les index de bloc et les jetons de bloc des blocs qui sont dans l'instantané `snap-0987654321`. Le paramètre `--starting-block-index` limite les résultats aux index de blocs supérieurs à 1000, et le paramètre `--max-results` limite les résultats aux premiers blocs 100.

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index 1000 --max-results 100
```

L'exemple de réponse suivant pour la commande précédente répertorie les index de bloc et les jetons de bloc dans l'instantané. Utilisez la commande `get-snapshot-block` et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```
{  
  "Blocks": [  

```

```

    {
      "BlockIndex": 1001,
      "BlockToken": "AAABAV3/
PNhX0ynVdMYHUpPsetaSvjLB1dtIGfbJv50J0sX855EzGTWos4a4"
    },
    {
      "BlockIndex": 1002,
      "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
    },
    {
      "BlockIndex": 1007,
      "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07e0gTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
    },
    {
      "BlockIndex": 1012,
      "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
    },
    {
      "BlockIndex": 1030,
      "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
    },
    {
      "BlockIndex": 1031,
      "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBCLkw6spzCxJVqDVAtskJ"
    },
    ...
  ],
  "ExpiryTime": 1576287332.806,
  "VolumeSize": 32212254720,
  "BlockSize": 524288
}

```

AWS API

L'[ListSnapshotBlocks](#) exemple de demande suivant renvoie les index de bloc et les jetons de bloc des blocs qui se trouvent dans SnapshotSnap-0acEXAMPLEcf41648. Le paramètre `startingBlockIndex` limite les résultats aux index de blocs supérieurs à 1000, et le paramètre `maxResults` limite les résultats aux premiers blocs 100.

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T231953Z
Authorization: <Authentication parameter>
```

L'exemple de réponse suivant pour la demande précédente répertorie les index de bloc et les jetons de bloc dans l'instantané. Utilisez l' `GetSnapshotBlock` action et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```
HTTP/1.1 200 OK
x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
Content-Type: application/json
Content-Length: 2472
Date: Wed, 17 Jun 2020 23:19:56 GMT
Connection: keep-alive

{
  "BlockSize": 524288,
  "Blocks": [
    {
      "BlockIndex": 0,
      "BlockToken": "AAUBACuWq0CnDNuK1e11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
    },
    {
      "BlockIndex": 1536,
      "BlockToken": "AAUBAWudwfmofcrQhGV1LwuRkm2b8ZXPIyrgoykTRC6IU1NbxKWDY1pPjvnV"
    },
    {
      "BlockIndex": 3072,
      "BlockToken": "AAUBAV7p6pC5fKAC7TokONCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
    },
    {
      "BlockIndex": 3073,
      "BlockToken": "AAUBAbqt9zpqBUEvt02HINAFaWTo0w1PjbIsQ01x6JUN/0+iMQ10NtNbnX4"
```



```
    },  
    ...  
  ],  
  "ExpiryTime": 1.59298379649E9,  
  "VolumeSize": 3  
}
```

Liste des blocs qui sont différents entre deux instantanés

Tenez compte des points suivants lorsque vous effectuez des demandes paginées pour répertorier les blocs modifiés entre deux instantanés :

- La réponse peut inclure un ou plusieurs tableaux `ChangedBlocks` vides. Par exemple :
 - Instantané 1 – instantané complet avec 1 000 blocs avec des index de blocs 0 – 999.
 - Instantané 2 – instantané incrémentiel avec un seul bloc modifié avec l'index de bloc 999.

La liste des blocs modifiés pour ces instantanés avec `StartingBlockIndex = 0` et `MaxResults = 100` renvoie un tableau vide de `ChangedBlocks`. Vous devez demander les autres résultats en utilisant `nextToken` jusqu'à ce que le bloc modifié soit retourné dans le dixième jeu de résultats, qui comprend les blocs avec les index de bloc 900 – 999.

- La réponse peut ignorer les blocs non écrits dans les instantanés. Par exemple :
 - Instantané 1 – instantané complet avec 1 000 blocs avec des index de blocs 2000 – 2999.
 - Instantané 2 – instantané incrémentiel avec un seul bloc modifié avec l'index de bloc 2000.

En listant les blocs modifiés pour ces instantanés avec `StartingBlockIndex = 0` et `MaxResults = 100`, la réponse ignore les index de bloc 0 – 1999 et inclut l'index de bloc 2000. La réponse n'inclura pas les tableaux `ChangedBlocks` vides.

AWS CLI

L'exemple de commande [list-changed-blocks](#) suivant renvoie les index de bloc et les jetons de bloc des blocs qui sont différents entre les instantanés `snap-1234567890` et `snap-0987654321`. Le paramètre `--starting-block-index` limite les résultats aux index de blocs supérieurs à 0, et le paramètre `--max-results` limite les résultats aux premiers blocs 500.

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-id snap-0987654321 --starting-block-index 0 --max-results 500
```

L'exemple de réponse suivant pour la commande précédente montre que les index de bloc 0, 6000, 6001, 6002 et 6003 sont différents entre les deux instantanés. De plus, les index de bloc 6001, 6002 et 6003 existent uniquement dans le premier ID d'instantané spécifié, et pas dans le second ID d'instantané car la réponse ne répertorie aucun second jeton de bloc.

Utilisez la commande `get-snapshot-block` et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```
{
  "ChangedBlocks": [
    {
      "BlockIndex": 0,
      "FirstBlockToken": "AAABAVahm9S060Dyi00RySzn2ZjGjW/KN3uygG1S0Q0YWesbzBbDnX2dGpmC",
      "SecondBlockToken": "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGSr"
    },
    {
      "BlockIndex": 6000,
      "FirstBlockToken": "AAABAbYSiZvJ0/R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
      "SecondBlockToken": "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777e1D9oVR"
    },
    {
      "BlockIndex": 6001,
      "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
    },
    {
      "BlockIndex": 6002,
      "FirstBlockToken": "AAABASqX4/NWjvNceoyMULjcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
    },
    {
      "BlockIndex": 6003,
      "FirstBlockToken": "AAABASmJ005JxA0ce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBR0uICb2A"
    }
  ]
}
```

```

    },
    ...
  ],
  "ExpiryTime": 1576308931.973,
  "VolumeSize": 32212254720,
  "BlockSize": 524288,
  "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVa00zsPH/QM3Bi3zF//
06Mdi/BbJarBnp8h"
}

```

AWS API

L'[ListChangedBlocks](#) exemple de requête suivant renvoie les index de bloc et les jetons de bloc des blocs qui sont différents entre les instantanés `snap-0acEXAMPLEcf41648` et `snap-0c9EXAMPLE1b30e2f`. Le paramètre `startingBlockIndex` limite les résultats aux index de blocs supérieurs à 0, et le paramètre `maxResults` limite les résultats aux premiers blocs 500.

```

GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T232546Z
Authorization: <Authentication parameter>

```

L'exemple de réponse suivant pour la requête précédente montre que les index de bloc 0, 3072, 6002 et 6003 sont différents entre les deux instantanés. De plus, les index de bloc 6002 et 6003 existent uniquement dans le premier ID d'instantané spécifié, et pas dans le second ID d'instantané car la réponse ne répertorie aucun second jeton de bloc.

Utilisez l'action `GetSnapshotBlock` et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```

HTTP/1.1 200 OK
x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
Content-Type: application/json
Content-Length: 1456
Date: Wed, 17 Jun 2020 23:25:47 GMT
Connection: keep-alive

```

```
{
  "BlockSize": 524288,
  "ChangedBlocks": [
    {
      "BlockIndex": 0,
      "FirstBlockToken": "AAUBAVaWq0CnDNuKle11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+OJkL",
      "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3N0resCxn5R0+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
    },
    {
      "BlockIndex": 3072,
      "FirstBlockToken":
"AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZ0LEmeXLmHBf2R/Yb24MaS",
      "SecondBlockToken":
"AAUBARGCaufCqBRZC8tEkPYGGkSv3vqv0jJ2xKDi3ljDFiytUxBLXYgTmkid"
    },
    {
      "BlockIndex": 6002,
      "FirstBlockToken": "AAABASqX4/
NWjvNceoyMULjcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
    },
    {
      "BlockIndex": 6003,
      "FirstBlockToken":
"AAABASmJ005JxA0ce25rF4P1sdRtyIDsX12tFEDunnePYUK0f4PBR0uICb2A"
    },
    ...
  ],
  "ExpiryTime": 1.592976647009E9,
  "VolumeSize": 3
}
```

Obtenir des données de bloc à partir d'un instantané

AWS CLI

L'exemple de commande [get-snapshot-block](#) suivant renvoie les données de l'index de bloc 6001 avec le jeton de bloc AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR, dans l'instantané snap-1234567890. Les données binaires seront générées dans le fichier `data` dans le répertoire `C:\Temp` sur un ordinateur

Windows. Si vous exécutez la commande sur un ordinateur Linux ou Unix, remplacez le chemin de sortie par `/tmp/data` pour générer les données dans le fichier `data` du répertoire `/tmp`.

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

L'exemple de réponse suivant pour la commande précédente montre la taille des données renvoyées, la somme de contrôle pour valider les données et l'algorithme de la somme de contrôle. Les données binaires sont automatiquement enregistrées dans le répertoire et le fichier que vous avez spécifiés dans la commande de demande.

```
{
  "DataLength": "524288",
  "Checksum": "cf0Y6/Fn0oFa4VyjQP0a/iD0zhTf1PTKzxGv20KowXc=",
  "ChecksumAlgorithm": "SHA256"
}
```

AWS API

L'[GetSnapshotBlock](#) exemple de requête suivant renvoie les données de l'index de bloc 3072 avec le jeton de bloc `AAUBARGCaufCqBRZC8tEkPYGGkSv3vqv0jJ2xKDi3ljDFiytUxBLXYgTmkid`, dans un instantané `snap-0c9EXAMPLE1b30e2f`.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqv0jJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T232838Z
Authorization: <Authentication parameter>
```

L'exemple de réponse suivant pour la demande précédente montre la taille des données renvoyées, la somme de contrôle pour valider les données et l'algorithme utilisé pour générer la somme de contrôle. Les données binaires sont transmises dans le corps de la réponse et sont représentées comme **BlockData** dans l'exemple suivant.

```
HTTP/1.1 200 OK
x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
```

```
x-amz-Data-Length: 524288
x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/octet-stream
Content-Length: 524288
Date: Wed, 17 Jun 2020 23:28:38 GMT
Connection: keep-alive
```

BlockData

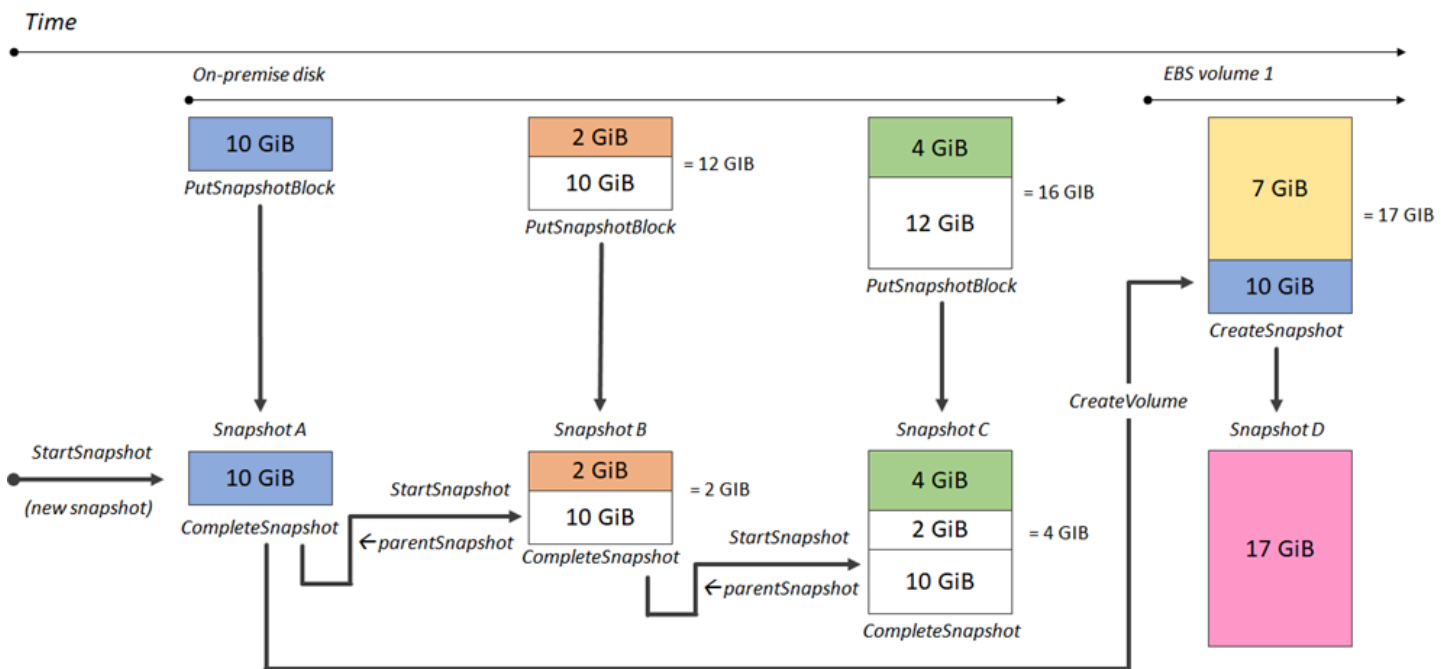
Rédigez des instantanés Amazon EBS avec les API EBS Direct

Les étapes suivantes décrivent comment utiliser des API directes EBS pour écrire des instantanés incrémentiels :

1. Utilisez cette StartSnapshot action et spécifiez un ID de cliché parent pour démarrer un instantané en tant que cliché incrémentiel d'un instantané existant, ou omettez l'ID de cliché parent pour démarrer un nouveau cliché. Cette action renvoie le nouvel ID d'instantané, qui est en attente.
2. Utilisez l' PutSnapshotBlock action et spécifiez l'ID de l'instantané en attente pour y ajouter des données sous forme de blocs individuels. Vous devez spécifier une somme de contrôle Base64-encoded SHA256 pour le bloc de données transmis. Le service calcule la somme de contrôle des données reçues et la valide avec la somme de contrôle que vous avez spécifiée. L'action échoue si les sommes de contrôle ne correspondent pas.
3. Lorsque vous avez terminé d'ajouter des données à l'instantané en attente, utilisez cette CompleteSnapshot action pour démarrer un flux de travail asynchrone qui scelle le cliché et le fait passer à l'état terminé.

Répétez ces étapes pour créer un nouvel instantané incrémentiel à l'aide de l'instantané précédemment créé en tant que parent.

Par exemple, dans le diagramme suivant, l'instantané A est le premier nouvel instantané démarré. L'instantané A est utilisé comme instantané parent pour démarrer l'instantané B. L'instantané B est utilisé comme instantané parent pour démarrer et créer l'instantané C. Les instantanés A, B et C sont des instantanés incrémentiels. L'instantané A est utilisé pour créer le volume EBS 1. L'instantané D est créé à partir du volume EBS 1. L'instantané D est un instantané incrémentiel de A ; et non un instantané incrémentiel de B ou C.



Les exemples suivants montrent comment écrire des instantanés à l'aide des API directes EBS.

Rubriques

- [Démarrer un instantané](#)
- [Ajouter des données dans un instantané](#)
- [Terminer un instantané](#)

Démarrer un instantané

AWS CLI

L'exemple de commande [start-snapshot](#) suivant démarre un instantané 8 Gio en utilisant l'instantané `snap-123EXAMPLE1234567` comme instantané parent. Le nouvel instantané sera un instantané incrémentiel de l'instantané parent. L'instantané passe à un état d'erreur s'il n'y a pas de demande d'ajout ou d'exécution pour l'instantané pendant la période de 60 minutes spécifiée. Le jeton client `550e8400-e29b-41d4-a716-446655440000` garantit l'idempotence pour la demande. Si le jeton client est omis, le AWS SDK en génère automatiquement un pour vous. Pour plus d'informations sur l'idempotence, consultez [Garantir l'idempotence dans StartSnapshot les requêtes d'API](#).

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

L'exemple de réponse suivant pour la commande précédente indique l'ID du snapshot, l'ID du compte AWS, l'état, la taille du volume en Gio et la taille des blocs dans l'instantané. L'instantané est démarré dans un état pending. Spécifiez l'ID d'instantané dans les commandes put-snapshot-block suivantes pour écrire des données dans l'instantané, puis utilisez la commande complete-snapshot pour terminer l'instantané et modifier son état sur completed.

```
{
  "SnapshotId": "snap-0aaEXAMPLEe306d62",
  "OwnerId": "111122223333",
  "Status": "pending",
  "VolumeSize": 8,
  "BlockSize": 524288
}
```

AWS API

L'[StartSnapshot](#) exemple de demande suivant démarre un instantané 8 GiB, en utilisant le snapshot snap-123EXAMPLE1234567 comme snapshot parent. Le nouvel instantané sera un instantané incrémentiel de l'instantané parent. L'instantané passe à un état d'erreur s'il n'y a pas de demande d'ajout ou d'exécution pour l'instantané pendant la période de 60 minutes spécifiée. Le jeton client 550e8400-e29b-41d4-a716-446655440000 garantit l'idempotence pour la demande. Si le jeton client est omis, le AWS SDK en génère automatiquement un pour vous. Pour plus d'informations sur l'idempotence, consultez [Garantir l'idempotence dans StartSnapshot les requêtes d'API](#).

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
  "VolumeSize": 8,
  "ParentSnapshot": snap-123EXAMPLE1234567,
  "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
  "Timeout": 60
}
```



```
}
```

L'exemple de réponse suivant pour la demande précédente indique l'ID d'instantané, l'ID de compte AWS, l'état, la taille du volume en Gio et la taille des blocs dans l'instantané. L'instantané est démarré dans un état en attente. Spécifiez l'ID d'instantané dans une demande PutSnapshotBlocks ultérieure d'écriture de données dans l'instantané.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
  "BlockSize": 524288,
  "Description": null,
  "OwnerId": "138695307491",
  "Progress": null,
  "SnapshotId": "snap-052EXAMPLEc85d8dd",
  "StartTime": null,
  "Status": "pending",
  "Tags": null,
  "VolumeSize": 8
}
```

Ajouter des données dans un instantané

AWS CLI

L'[exemple de commande](#) put-snapshot-block suivant écrit des 524288 octets de données pour bloquer l'index sur l'instantané. 1000 snap-0aaEXAMPLEe306d62 La somme de contrôle Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM= codée en Base64 a été générée à l'aide de l'algorithme SHA256. Les données transmises se trouvent dans le fichier /tmp/data.

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
--block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM= --checksum-algorithm SHA256
```

L'exemple de réponse suivant pour la commande précédente confirme la longueur des données, la somme de contrôle et l'algorithme de somme de contrôle pour les données reçues par le service.

```
{
  "DataLength": "524288",
  "Checksum": "Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=",
  "ChecksumAlgorithm": "SHA256"
}
```

AWS API

L'[PutSnapshot](#) exemple de requête suivant écrit des 524288 octets de données pour bloquer l'index 1000 sur l'instantané `snap-052EXAMPLEc85d8dd`. La somme de contrôle `Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=` codée en Base64 a été générée à l'aide de l'algorithme SHA256. Les données sont transmises dans le corps de la demande et sont représentées comme *BlockData* dans l'exemple suivant.

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>
```

BlockData

Voici un exemple de réponse pour la demande précédente, qui confirme la longueur des données, la somme de contrôle et l'algorithme de somme de contrôle pour les données que le service reçoit.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: Q0D3gmEQ0XATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
```

```
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

{}
```

Terminer un instantané

AWS CLI

L'exemple de commande [complete-snapshot](#) suivant termine l'instantané `snap-0aaEXAMPLEe306d62`. La commande spécifie que les blocs 5 ont été écrits dans l'instantané. La somme de contrôle `6D3nmwi5f2F0wlh7xX8QprJBFzDX8aacd0cA3KCM3c=` représente la somme de contrôle de l'ensemble complet des données écrites dans un instantané. Pour plus d'informations sur les sommes de contrôle, consultez [Utilisez les sommes de contrôle des API directes EBS pour valider les données des instantanés](#) plus haut dans ce guide.

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-
count 5 --checksum 6D3nmwi5f2F0wlh7xX8QprJBFzDX8aacd0cA3KCM3c= --checksum-
algorithm SHA256 --checksum-aggregation-method LINEAR
```

Voici un exemple de réponse pour la commande précédente.

```
{
  "Status": "pending"
}
```

AWS API

L'[CompleteSnapshot](#) exemple de demande suivant complète le `snapshotsnap-052EXAMPLEc85d8dd`. La commande spécifie que les blocs 5 ont été écrits dans l'instantané. La somme de contrôle `6D3nmwi5f2F0wlh7xX8QprJBFzDX8aacd0cA3KCM3c=` représente la somme de contrôle de l'ensemble complet des données écrites dans un instantané.

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprJBFzDX8aacd0cA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
```

```
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

Voici un exemple de réponse pour la demande précédente.

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

Résultats du chiffrement pour les API EBS Direct

Lorsque vous démarrez un nouveau snapshot à l'aide de [StartSnapshot](#), l'état du chiffrement dépend des valeurs que vous spécifiez pour `Encrypted`, `KmsKeyArn`, et `ParentSnapshotId`, et si le [chiffrement est activé par défaut sur votre AWS compte](#).

Note

- Vous pouvez avoir besoin d'autorisations IAM supplémentaires pour utiliser le API directes EBS avec le chiffrement. Pour plus d'informations, consultez [Autorisations d'utilisation AWS KMS keys](#).
- Si le chiffrement Amazon EBS est activé par défaut sur votre AWS compte, vous ne pouvez pas créer d'instantanés non chiffrés.
- Si le chiffrement Amazon EBS est activé par défaut sur votre AWS compte, vous ne pouvez pas créer un nouvel instantané à l'aide d'un instantané parent non chiffré. Vous devez d'abord chiffrer l'instantané parent en le copiant. Pour plus d'informations, consultez [Copier un instantané Amazon EBS](#).

Rubriques

- [Résultats du chiffrement : instantané parent non chiffré](#)
- [Résultats du chiffrement : instantané parent chiffré](#)

- [Résultats du chiffrement : aucun instantané parent](#)

Résultats du chiffrement : instantané parent non chiffré

Le tableau suivant décrit le résultat du chiffrement pour chaque combinaison possible de paramètres lors de la spécification d'un instantané parent non chiffré.

ParentSnapshotId	Encrypted	KmsKeyArn	Chiffrement par défaut	Résultat
Non chiffré	Omis	Omis	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	L'instantané n'est pas chiffré.
		Spécifié	Activé	
			Désactivé	
Non chiffré	True	Omis	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	
		Spécifié	Activé	
			Désactivé	
Non chiffré	False	Omis	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	
		Spécifié	Activé	
			Désactivé	

Résultats du chiffrement : instantané parent chiffré

Le tableau suivant décrit le résultat du chiffrement pour chaque combinaison possible de paramètres lors de la spécification d'un instantané parent chiffré.

ParentSnapshotId	Encrypted	KmsKeyArn	Chiffrement par défaut	Résultat
Encrypted	Omis	Omis	Activé	L'instantané est chiffré à l'aide de la même clé KMS que l'instantané parent.
			Désactivé	
		Spécifié	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	
Encrypted	True	Omis	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	
		Spécifié	Activé	
			Désactivé	
Encrypted	False	Omis	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	
		Spécifié	Activé	
			Désactivé	

Résultats du chiffrement : aucun instantané parent

Les tableaux suivants décrivent le résultat du chiffrement pour chaque combinaison possible de paramètres en l'absence d'utilisation d'un instantané parent.

ParentSnapshotId	Encrypted	KmsKeyArn	Chiffrement par défaut	Résultat
Omis	True	Omis	Activé	L'instantané est chiffré à l'aide de la clé KMS par défaut de votre compte. *
			Désactivé	

ParentSnapshotId	Encrypted	KmsKeyArn	Chiffrement par défaut	Résultat
Omis	False	Spécifié	Activé	L'instantané est chiffré à l'aide de la clé KMS spécifiée pour KmsKeyArn.
			Désactivé	
		Omis	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	L'instantané n'est pas chiffré.
Omis	Omis	Spécifié	Activé	Échec de la demande avec <code>ValidationException</code> .
			Désactivé	
		Omis	Activé	L'instantané est chiffré à l'aide de la clé KMS par défaut de votre compte. *
			Désactivé	L'instantané n'est pas chiffré.
		Spécifié	Activé	L'instantané est chiffré à l'aide de la clé KMS spécifiée pour KmsKeyArn.
			Désactivé	

* Cette clé KMS par défaut peut être une clé gérée par le client ou la clé KMS AWS gérée par défaut pour le chiffrement Amazon EBS.

Utilisez les sommes de contrôle des API directes EBS pour valider les données des instantanés

L' `GetSnapshotBlock` action renvoie les données qui se trouvent dans un bloc d'un instantané, et l' `PutSnapshotBlock` action ajoute des données à un bloc d'un instantané. Les données de bloc transmises ne sont pas signées dans le cadre du processus de signature de la version 4. Par conséquent, les sommes de contrôle sont utilisées pour valider l'intégrité des données comme suit :

- Lorsque vous utilisez cette `GetSnapshotBlock` action, la réponse fournit une somme de contrôle Base64-encoded SHA256 pour les données du bloc à l'aide de l'en-tête `X-AMZ-Checksum`, et l'algorithme de somme de contrôle à l'aide de l'en-tête `x-amz-Checksum-Algorithm`. Utilisez la somme de contrôle renvoyée pour valider l'intégrité des données. Si la somme de contrôle que vous générez ne correspond pas à celle fournie par Amazon EBS, vous devez considérer les données non valides et réessayer votre demande.
- Lorsque vous utilisez cette `PutSnapshotBlock` action, votre demande doit fournir une somme de contrôle Base64-encoded SHA256 pour les données de bloc à l'aide de l'en-tête `X-AMZ-Checksum` et l'algorithme de somme de contrôle utilisant l'en-tête `x-amz-Checksum-Algorithm`. La somme de contrôle que vous fournissez est validée par rapport à une somme de contrôle générée par Amazon EBS pour valider l'intégrité des données. Si les sommes de contrôle ne correspondent pas, la demande échoue.
- Lorsque vous utilisez cette `CompleteSnapshot` action, votre demande peut éventuellement fournir une somme de contrôle Base64-encoded SHA256 agrégée pour l'ensemble complet des données ajoutées à l'instantané. Fournissez la somme de contrôle à l'aide de l'en-tête `X-AMZ-Checksum`, l'algorithme de somme de contrôle à l'aide de l'en-tête `x-amz-Checksum-Algorithm` et la méthode d'agrégation des sommes de contrôle à l'aide de l'en-tête `x-amz-Checksum-Aggregation-Method`. Pour générer la somme de contrôle agrégée à l'aide de la méthode d'agrégation linéaire, organisez les sommes de contrôle pour chaque bloc écrit dans l'ordre croissant de leur index de bloc, concaténez-les pour former une seule chaîne, puis générez la somme de contrôle sur la chaîne entière à l'aide de l'algorithme SHA256.

Les sommes de contrôle de ces actions font partie du processus de signature de la version 4.

Garantir l'idempotence dans `StartSnapshot` les requêtes d'API

L'idempotence garantit qu'une requête API n'est exécutée qu'une seule fois. Avec une demande idempotente, si la demande d'origine se termine avec succès, les tentatives suivantes renvoient le résultat de la demande d'origine réussie et elles n'ont aucun effet supplémentaire.

L' [StartSnapshot](#) API prend en charge l'idempotence à l'aide d'un jeton client. Un jeton client est une chaîne unique que vous spécifiez lorsque vous effectuez une demande d'API. Si vous réessayez une demande d'API avec le même jeton client et les mêmes paramètres de requête une fois qu'elle est terminée correctement, le résultat de la demande d'origine est renvoyé. Si vous réessayez une demande avec le même jeton client, mais que vous modifiez un ou plusieurs paramètres de requête, l'erreur `ConflictException` est renvoyée.

Si vous ne spécifiez pas votre propre jeton client, les AWS SDK génèrent automatiquement un jeton client pour la demande afin de s'assurer qu'elle est idempotente.

Un jeton client peut être n'importe quelle chaîne qui comprend jusqu'à 64 caractères ASCII. Vous ne devez pas réutiliser les mêmes jetons client pour différentes demandes.

Pour effectuer une StartSnapshot demande idempotente avec votre propre jeton client à l'aide de l'API

Spécifiez le paramètre de demande ClientToken.

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
  "VolumeSize": 8,
  "ParentSnapshot": snap-123EXAMPLE1234567,
  "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
  "Timeout": 60
}
```

Pour effectuer une StartSnapshot demande idempotente avec votre propre jeton client à l'aide du AWS CLI

Spécifiez le paramètre de demande client-token.

```
$ C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-
snapshot snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-
a716-446655440000
```

Rétentatives d'erreur pour les API EBS Direct

Les AWS kits SDK implémente une logique de nouvelle tentative automatique pour les demandes renvoyant des réponses d'erreur. Vous pouvez configurer les paramètres de nouvelle tentative pour les kits SDK AWS . Pour plus d'informations, consultez la documentation de votre kit SDK.

Vous pouvez configurer AWS CLI pour réessayer automatiquement certaines demandes qui ont échoué. Pour plus d'informations sur la configuration des nouvelles tentatives pour le AWS CLI, voir les nouvelles [AWS CLI tentatives](#) dans le Guide de l'AWS Command Line Interface utilisateur.

L'AWS API de requête ne prend pas en charge la logique de nouvelle tentative pour les demandes ayant échoué. Si vous utilisez des requêtes HTTP ou HTTPS, vous devez implémenter une logique de nouvelle tentative dans votre application cliente.

Le tableau suivant présente les réponses possibles aux erreurs de l'API. Certaines erreurs de l'API peuvent faire l'objet d'une nouvelle tentative. Votre application client doit toujours relancer les demandes qui ont échoué et qui reçoivent une erreur récupérable.

Erreur	Code de réponse	Description	Lancé par	Récupérable ?
InternalServerException	500	La demande a échoué en raison d'un problème réseau ou AWS côté serveur.	Toutes les API	Oui
ThrottlingException	400	Le nombre de demandes d'API a dépassé la limite maximale de limitation des demandes d'API autorisée pour le compte.	Toutes les API	Oui
RequestThrottledException	400	Le nombre de demandes d'API a dépassé la limite maximale de limitation des demandes d'API autorisée pour l'instantané.	GetSnapshotBlock PutSnapshotBlock	Oui

Erreur	Code de réponse	Description	Lancé par	Récupérable ?
ValidationException avec le message « Failed to read block data »	400	Le bloc de données fourni n'était pas lisible.	PutSnapshotBlock	Oui
ValidationException avec tout autre message	400	La syntaxe de la demande est mal formée, ou l'entrée ne satisfait pas aux contraintes spécifiées par Service AWS.	Toutes les API	Non
ResourceNotFoundException	404	L'ID de l'instantané spécifié n'existe pas.	Toutes les API	Non

Erreur	Code de réponse	Description	Lancé par	Récupérable ?
ConflictException	409	Le jeton client spécifié a déjà été utilisé dans une demande similaire dont les paramètres étaient différents. Pour de plus amples informations, veuillez consulter Garantir l'idempotence dans StartSnapshot les requêtes d'API.	StartSnapshot	Non
AccessDeniedException	403	Vous n'avez pas l'autorisation d'effectuer l'opération demandée.	Toutes les API	Non
ServiceQuotaExceededException	402	La demande a échoué, car son exécution dépasserait un ou plusieurs quotas de services dépendants pour votre compte.	Toutes les API	Non

Erreur	Code de réponse	Description	Lancé par	Récupérable ?
InvalidSignatureException	403	La signature d'autorisation de la demande a expiré. Vous ne pouvez réessayer la demande qu'après avoir actualisé la signature d'autorisation.	Toutes les API	Non

Optimisez les performances des API EBS Direct

Vous pouvez exécuter des demandes d'API simultanément. En supposant que la PutSnapshotBlock latence soit de 100 ms, un thread peut traiter 10 requêtes en une seconde. En outre, en supposant que votre application cliente crée plusieurs threads et connexions (par exemple, 100 connexions), elle peut faire 1000 (10 * 100) demandes par seconde au total. Cela correspondra à un débit d'environ 500 Mo par seconde.

La liste suivante contient quelques éléments à rechercher dans votre application :

- Chaque thread utilise-t-il une connexion séparée ? Si les connexions sont limitées sur l'application, plusieurs threads attendront que la connexion soit disponible et vous remarquerez un débit inférieur.
- Y a-t-il un temps d'attente dans l'application entre deux demandes d'ajout ? Cela réduira le débit effectif d'un thread.
- Limite de bande passante sur l'instance : si la bande passante de l'instance est partagée par d'autres applications, cela peut limiter le débit disponible pour les PutSnapshotBlock requêtes.

Veillez à prendre note des autres charges de travail qui peuvent être exécutées dans le compte pour éviter les goulots d'étranglement. Vous devez également créer des mécanismes de nouvelle tentative dans vos flux de travail API directes EBS afin de gérer la limitation, les délais d'attente et l'indisponibilité du service.

Passez en revue les quotas de service API directes EBS pour déterminer le maximum de demandes d'API que vous pouvez exécuter par seconde. Pour plus d'informations, consultez [Points de terminaison et quotas Amazon Elastic Block Store](#) dans AWS General Reference.

Points de terminaison de service pour les API EBS Direct

Un point de terminaison est une URL qui sert de point d'entrée à un service AWS Web. Les API directes EBS prennent en charge les types de point de terminaison suivants :

- Points de terminaison IPv4
- Dual-stack terminaux prenant en charge à la fois IPv4 et IPv6
- Points de terminaison FIPS

Lorsque vous faites une demande, vous pouvez spécifier le point de terminaison et la région à utiliser. Si vous ne spécifiez pas de point de terminaison, le point de terminaison IPv4 est utilisé par défaut. Pour utiliser un autre type de point de terminaison, vous devez le spécifier dans votre demande. Pour obtenir un exemple de la façon de procéder, consultez [Spécification des points de terminaison](#).

Pour plus d'informations sur les régions, consultez la section [Régions et zones de disponibilité](#) dans le guide de l'utilisateur Amazon EC2. Pour obtenir une liste des points de terminaison des API directes EBS, consultez [Points de terminaison pour les API directes EBS](#) dans la Référence générale d'Amazon Web Services.

Rubriques

- [Points de terminaison IPv4](#)
- [Dual-stack points de terminaison \(IPv4 et IPv6\)](#)
- [Points de terminaison FIPS](#)
- [Spécification des points de terminaison](#)

Points de terminaison IPv4

Les points de terminaison IPv4 prennent en charge le trafic IPv4 uniquement. Les points de terminaison IPv4 sont disponibles pour toutes les régions.

Les API EBS direct ne prennent en charge que les points de terminaison IPv4 régionaux que vous pouvez utiliser pour effectuer vos demandes. Vous devez spécifier la région dans le nom du point de terminaison. Les noms des points de terminaison utilisent la convention de dénomination suivante :

- `ebs.region.amazonaws.com`

Par exemple, pour diriger vos demandes vers le point de terminaison us-east-2 IPv4, vous devez spécifier `ebs.us-east-2.amazonaws.com` comme point de terminaison. Pour obtenir une liste des points de terminaison des API directes EBS, consultez [Points de terminaison pour les API directes EBS](#) dans la Référence générale d'Amazon Web Services.

Tarification

Vous n'êtes pas facturé pour les données transférées directement entre les API directes EBS et les instances Amazon EC2 utilisant un point de terminaison IPv4 dans la même région. Toutefois, s'il existe des services intermédiaires, tels que des AWS PrivateLink points de terminaison, NAT Gateway ou Amazon VPC Transit Gateways, les coûts associés vous sont facturés.

Dual-stack points de terminaison (IPv4 et IPv6)

Dual-stack les terminaux prennent en charge le trafic IPv4 et IPv6. Dual-stack les points de terminaison sont disponibles pour toutes les régions.

Pour utiliser IPv6, vous devez utiliser un point de terminaison à double pile. Lorsque vous adressez une requête à un point de terminaison à double pile, l'URL du point de terminaison se résout en une adresse IPv6 ou IPv4, selon le protocole utilisé par votre réseau et votre client.

Les API EBS direct ne prennent en charge que les points de terminaison régionaux à double pile, ce qui signifie que vous devez spécifier la région dans le nom du point de terminaison. Dual-stack les noms de points de terminaison utilisent la convention de dénomination suivante :

- `ebs.region.api.aws`

Par exemple, le nom du point de terminaison à double pile de la région eu-west-1 est `ebs.eu-west-1.api.aws`. Pour obtenir une liste des points de terminaison des API directes EBS, consultez [Points de terminaison pour les API directes EBS](#) dans la Référence générale d'Amazon Web Services.

Tarification

Vous n'êtes pas facturé pour les données transférées directement entre les API directes EBS et les instances Amazon EC2 utilisant un point de terminaison à double pile dans la même région. Toutefois, s'il existe des services intermédiaires, tels que des AWS PrivateLink points de terminaison, NAT Gateway ou Amazon VPC Transit Gateways, les coûts associés vous sont facturés.

Points de terminaison FIPS

Les API EBS Direct fournissent des points de terminaison FIPS-validated IPv4 et à double pile (IPv4 et IPv6) pour les régions suivantes :

- `us-east-1` : USA Est (Virginie du Nord)
- `us-east-2` : USA Est (Ohio)
- `us-west-1` : USA Ouest (Californie du Nord)
- `us-west-2` : USA Ouest (Oregon)
- `ca-central-1` : Canada (Centre)
- `ca-west-1`— Canada-Ouest (Calgary)

Les points de terminaison IPv4 FIPS utilisent la convention d'affectation de noms suivante : `ebs-fips.region.amazonaws.com`. Par exemple, le point de terminaison IPv4 FIPS pour `us-east-1` est `ebs-fips.us-east-1.amazonaws.com`.

Les points de terminaison FIPS à double pile utilisent la convention d'affectation de noms suivante : `ebs-fips.region.api.aws`. Par exemple, le point de terminaison à double pile FIPS pour `us-east-1` est `ebs-fips.us-east-1.api.aws`.

Pour plus d'informations sur les points de terminaison FIPS, consultez [Points de terminaison FIPS](#) dans le Référence générale d'Amazon Web Services.

Spécification des points de terminaison

Cette section fournit quelques exemples sur la manière de spécifier un point de terminaison lors de l'envoi d'une demande.

AWS CLI

Les exemples suivants montrent comment spécifier un point de terminaison pour la région `us-east-2` à l'aide de AWS CLI.

- Dual-stack


```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
1000 --endpoint-url https://ebs.us-east-2.api.aws
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
1000 --endpoint-url https://ebs.us-east-2.amazonaws.com
```

AWS SDK for Java 2.x

Les exemples suivants montrent comment spécifier un point de terminaison pour la région us-east-2 à l'aide de AWS SDK for Java 2.x.

- Dual-stack

```
AwsClientBuilder.EndpointConfiguration config = new
    AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.api.aws", "us-
east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new
    AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.amazonaws.com",
    "us-east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

AWS SDK for Go

Les exemples suivants montrent comment spécifier un point de terminaison pour la région us-east-2 à l'aide de AWS SDK pour Go.

- Dual-stack

```
sess := session.Must(session.NewSession())
```

```
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast2RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.api.aws")
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast2RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.amazonaws.com")
})
```

AWS Exemples de code SDK pour les API EBS Direct

Les exemples de code suivants montrent comment utiliser les API EBS Direct avec un kit de développement AWS logiciel (SDK).

Actions

- [À utiliser StartSnapshot avec AWS SDK ou CLI](#)
- [À utiliser PutSnapshotBlock avec un AWS SDK ou CLI](#)
- [À utiliser CompleteSnapshot avec un AWS SDK ou CLI](#)

À utiliser **StartSnapshot** avec AWS SDK ou CLI

L'exemple de code suivant montre comment utiliser `StartSnapshot`.

Rust

SDK pour Rust

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](#).

```
async fn start(client: &Client, description: &str) -> Result<String, Error> {
```

```

    let snapshot = client
        .start_snapshot()
        .description(description)
        .encrypted(false)
        .volume_size(1)
        .send()
        .await?;

    Ok(snapshot.snapshot_id.unwrap())
}

```

- Pour plus de détails sur l'API, consultez [StartSnapshot](#) la section Référence de l'API AWS SDK pour Rust.

À utiliser **PutSnapshotBlock** avec un AWS SDK ou CLI

L'exemple de code suivant montre comment utiliser `PutSnapshotBlock`.

Rust

SDK pour Rust

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](#).

```

async fn add_block(
    client: &Client,
    id: &str,
    idx: usize,
    block: Vec<u8>,
    checksum: &str,
) -> Result<(), Error> {
    client
        .put_snapshot_block()
        .snapshot_id(id)
        .block_index(idx as i32)
        .block_data(ByteStream::from(block))

```

```

        .checksum(checksum)
        .checksum_algorithm(ChecksumAlgorithm::ChecksumAlgorithmSha256)
        .data_length(EBS_BLOCK_SIZE as i32)
        .send()
        .await?;

    Ok(())
}

```

- Pour plus de détails sur l'API, consultez [PutSnapshotBlock](#) la section Référence de l'API AWS SDK pour Rust.

À utiliser **CompleteSnapshot** avec un AWS SDK ou CLI

L'exemple de code suivant montre comment utiliser `CompleteSnapshot`.

Rust

SDK pour Rust

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](#).

```

async fn finish(client: &Client, id: &str) -> Result<(), Error> {
    client
        .complete_snapshot()
        .changed_blocks_count(2)
        .snapshot_id(id)
        .send()
        .await?;

    println!("Snapshot ID {}", id);
    println!("The state is 'completed' when all of the modified blocks have been
transferred to Amazon S3.");
    println!("Use the get-snapshot-state code example to get the state of the
snapshot.");
}

```

```
    ok(() )  
}
```

- Pour plus de détails sur l'API, consultez [CompleteSnapshot](#) la section Référence de l'API AWS SDK pour Rust.

Création d'une connexion privée entre un VPC et les API directes EBS

Vous pouvez établir une connexion privée entre votre VPC et les API directes EBS en créant un point de terminaison de VPC d'interface, optimisé par [AWS PrivateLink](#). Vous pouvez accéder aux API directes EBS comme si le service se trouvait dans votre VPC, sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC ne nécessitent pas d'adresses IP publiques pour communiquer avec les API directes EBS.

Nous créons une interface réseau du point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface.

Pour plus d'informations, consultez la section [Accès Services AWS via AWS PrivateLink](#) le AWS PrivateLink Guide.

Considérations relatives aux points de terminaison VPC des API directes EBS

Avant de configurer un point de terminaison d'un VPC d'interface pour les API directes EBS, consultez [Considérations](#) dans le Guide AWS PrivateLink.

Par défaut, l'accès complet aux API directes EBS est autorisé via le point de terminaison. Vous pouvez contrôler l'accès au point de terminaison de l'interface à l'aide des politiques de point de terminaison VPC. Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès aux API EBS Direct. La politique spécifie les informations suivantes :

- Le `principal` qui peut effectuer des actions.
- Les `actions` qui peuvent être effectuées.
- Les `ressources` sur lesquelles les actions peuvent être effectuées.

Pour de plus amples informations, veuillez consulter [Contrôle de l'accès aux services avec points de terminaison d'un VPC](#) dans le Amazon VPC Guide de l'utilisateur.

Voici un exemple de politique de point de terminaison pour les API EBS Direct. Lorsqu'elle est associée à un endpoint, cette politique donne accès à toutes les actions directes des API EBS sur toutes les ressources, à l'exception des instantanés marqués par une clé Environment et une valeur. Test

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ebs:*",
      "Principal": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Environment": "Test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ebs:*",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

Créer un point de terminaison d'un VPC d'interface pour les API directes EBS

Vous pouvez créer un point de terminaison d'un VPC pour des API directes EBS à l'aide de la console Amazon VPC ou de l' AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez [Créer un point de terminaison d'un VPC](#) dans le Guide AWS PrivateLink .

Créez un point de terminaison VPC pour les API EBS Direct en utilisant l'un des noms de service suivants :

- com.amazonaws.*region*.ebs

- `com.amazonaws.region.ebs-fips`— Créer un point de terminaison VPC d'interface conforme à la norme gouvernementale américaine FIPS (Federal Information Processing Standard) Publication 140-2.

Note

FIPS-compliant interface Les points de terminaison VPC peuvent être créés pour les régions suivantes : `us-east-1` | `us-east-2` | `us-west-1` | `us-west-2` | `ca-central-1` | `ca-west-1` FIPS-compliant interface Les points de terminaison VPC prennent en charge à la fois le trafic IPv4 et IPv6.

Si vous activez le DNS privé pour le point de terminaison, vous pouvez faire des demandes d'API vers les API directes EBS en utilisant le nom DNS par défaut pour la région, par exemple `ebs.us-east-1.amazonaws.com`.

Enregistrez les appels d'API directs EBS à l'aide de AWS CloudTrail

Les API EBS Direct sont intégrées à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture les appels effectués vers les API directes d'EBS sous forme d'événements. Les appels capturés incluent les appels en provenance des API EBS Direct Console de gestion AWS et les appels de code vers les API EBS Direct. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite aux API EBS Direct, 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 votre 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. L'affichage de CloudTrail l'historique des événements est gratuit.

Pour un enregistrement continu des événements survenus au cours de vos 90 Compte AWS derniers jours, créez un trail ou une banque de données sur les [événements](#) CloudTrail Lake.

CloudTrail sentiers

Un journal permet CloudTrail de transmettre 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 historique multirégional, car vous pouvez enregistrer 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 gratuitement une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 CloudTrail en créant un historique, mais 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 Magasins de données sur les événements liés

CloudTrail Lake vous permet de lancer SQL-based des requêtes 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 [Utilisation de AWS CloudTrail Lake](#) dans le Guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et les requêtes de données sur les événements liés aux lacs 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](#).

EBS dirige les événements de données des API dans CloudTrail

[Les événements de données](#) fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource. 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 ressources des API EBS Direct à l'aide de la CloudTrail console ou AWS CLI des opérations CloudTrail d'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 .

Vous pouvez enregistrer les opérations des API directes EBS suivantes en tant qu'événements de données.

- [ListSnapshotBlocks](#)
- [ListChangedBlocks](#)
- [GetSnapshotBlock](#)
- [PutSnapshotBlock](#)

Note

Si vous effectuez une action sur un instantané partagé avec vous, les événements liés aux données ne sont pas envoyés au AWS compte propriétaire de l'instantané.

Événements de gestion directe des API EBS 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.

Le service EBS direct APIs enregistre les opérations suivantes du plan de contrôle en CloudTrail tant qu'événements de gestion.

- [StartSnapshot](#)
- [CompleteSnapshot](#)

Exemples d'événements liés aux API EBS Direct

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 pile ordonnée des appels d'API publics, de sorte que les événements n'apparaissent pas dans un ordre spécifique.

Voici des exemples d' CloudTrail événements pour les API EBS Direct.

StartSnapshot

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
```

```

"eventTime": "2020-07-03T23:27:26Z",
"eventSource": "ebs.amazonaws.com",
"eventName": "StartSnapshot",
"awsRegion": "eu-west-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "PostmanRuntime/7.25.0",
"requestParameters": {
  "volumeSize": 8,
  "clientToken": "token",
  "encrypted": true
},
"responseElements": {
  "snapshotId": "snap-123456789012",
  "ownerId": "123456789012",
  "status": "pending",
  "startTime": "Jul 3, 2020 11:27:26 PM",
  "volumeSize": 8,
  "blockSize": 524288,
  "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
"eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}

```

CompleteSnapshot

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2020-07-03T23:28:24Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "CompleteSnapshot",
  "awsRegion": "eu-west-1",
  "sourceIPAddress": "192.0.2.0",

```

```

    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
      "snapshotId": "snap-123456789012",
      "changedBlocksCount": 5
    },
    "responseElements": {
      "status": "completed"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
  }

```

ListSnapshotBlocks

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAT4HPB2A03JEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2021-06-03T00:32:46Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "ListSnapshotBlocks",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "111.111.111.111",
  "userAgent": "PostmanRuntime/7.28.0",
  "requestParameters": {
    "snapshotId": "snap-abcdef01234567890",
    "maxResults": 100,
    "startingBlockIndex": 0
  },
  "responseElements": null,
  "requestID": "example6-0e12-4aa9-b923-1555eexample",
  "eventID": "example4-218b-4f69-a9e0-2357dexample",
  "readOnly": true,
  "resources": [
    {

```

```

        "accountId": "123456789012",
        "type": "AWS::EC2::Snapshot",
        "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
    },
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}

```

ListChangedBlocks

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2A03JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
}

```

```

"readOnly": true,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::EC2::Snapshot",
    "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
  },
  {
    "accountId": "123456789012",
    "type": "AWS::EC2::Snapshot",
    "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
  }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-SHA",
  "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
}
}

```

GetSnapshotBlock

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAT4HPB2A03JEXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "user"
  },
  "eventTime": "2021-06-02T20:43:05Z",
  "eventSource": "ebs.amazonaws.com",
  "eventName": "GetSnapshotBlock",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "111.111.111.111",
  "userAgent": "PostmanRuntime/7.28.0",
  "requestParameters": {

```

```

        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}

```

PutSnapshotBlock

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2A03JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "PutSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",

```

```

"userAgent": "PostmanRuntime/7.28.0",
"requestParameters": {
  "snapshotId": "snap-abcdef01234567890",
  "blockIndex": 1,
  "dataLength": 524288,
  "checksum": "exampleodSGvFSb1e3kxWUgb0Q4TbzPurnsfVexample",
  "checksumAlgorithm": "SHA256"
},
"responseElements": {
  "checksum": "exampleodSGvFSb1e3kxWUgb0Q4TbzPurnsfVexample",
  "checksumAlgorithm": "SHA256"
},
"requestID": "example3-d5e0-4167-8ee8-50845example",
"eventID": "example8-4d9a-4aad-b71d-bb31fexample",
"readOnly": false,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS::EC2::Snapshot",
    "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
  }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-SHA",
  "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
}
}

```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, consultez la section Contenu des [CloudTrail enregistrements](#) dans le Guide de AWS CloudTrail l'utilisateur.

Questions fréquemment posées sur les API EBS Direct

Est-il possible d'accéder à un instantané à l'aide des API directes EBS si son statut est en attente ?

Non. L'instantané n'est accessible que si son statut est terminé.

Les index de bloc sont-ils renvoyés par les API directes EBS dans l'ordre numérique ?

Oui. Les index de bloc renvoyés sont uniques et classés par ordre numérique.

Puis-je soumettre une demande avec une valeur de MaxResults paramètre inférieure à 100 ?

Non La valeur de MaxResult paramètre minimale que vous pouvez utiliser est 100. Si vous soumettez une demande avec une valeur de MaxResult paramètre inférieure à 100 et que l'instantané contient plus de 100 blocs, l'API renverra au moins 100 résultats.

Puis-je exécuter des demandes d'API simultanément ?

Vous pouvez exécuter des demandes d'API simultanément. Veillez à prendre note des autres charges de travail qui peuvent être exécutées dans le compte pour éviter les goulots d'étranglement. Vous devez également créer des mécanismes de nouvelle tentative dans vos flux de travail API directes EBS afin de gérer la limitation, les délais d'attente et l'indisponibilité du service. Pour plus d'informations, consultez [Optimisez les performances des API EBS Direct](#).

Passez en revue les quotas de service API directes EBS pour déterminer les demandes d'API que vous pouvez exécuter par seconde. Pour plus d'informations, consultez [Points de terminaison et quotas Amazon Elastic Block Store](#) dans AWS General Reference.

Lors de l'exécution de l' ListChangedBlocks action, est-il possible d'obtenir une réponse vide même s'il y a des blocs dans l'instantané ?

Oui. Si les blocs modifiés sont rares dans l'instantané, la réponse peut être vide, mais l'API renverra une valeur de jeton de page suivante. Utilisez la valeur de jeton de page suivante pour passer à la page suivante des résultats. Vous pouvez confirmer que vous avez atteint la dernière page de résultats lorsque l'API renvoie une valeur de jeton de page suivante nulle.

Si le NextToken paramètre est spécifié en même temps qu'un StartingBlockIndex paramètre, lequel des deux est utilisé ?

Le NextToken est utilisé et le StartingBlockIndex est ignoré.

Quelle est la durée de validité des jetons de bloc et des jetons suivants ?

Les jetons de bloc sont valides pendant sept jours et les jetons suivants sont valides pendant 60 minutes.

Les instantanés chiffrés sont-ils pris en charge ?

Oui. Les instantanés chiffrés sont accessibles à l'aide des API directes EBS.

Pour accéder à un instantané chiffré, vous devez avoir accès à la clé KMS utilisée pour chiffrer le cliché et à l'action de AWS KMS déchiffrement. Consultez la [Contrôlez l'accès aux API EBS Direct à l'aide d'IAM](#) section précédente de ce guide pour connaître la AWS KMS politique à attribuer à un utilisateur.

Les instantanés publics sont-ils pris en charge ?

Les instantanés publics ne sont pas pris en charge.

Les instantanés locaux d'Amazon EBS sont-ils pris en charge ? AWS Outposts

Les instantanés locaux Amazon EBS ne AWS Outposts sont pas pris en charge.

L'opération ListSnapshotBlocks renvoie-t-elle tous les index de bloc et tous les jetons de bloc d'un instantané, ou seulement ceux dans lesquels des données ont été écrites ?

Elle renvoie uniquement les index de bloc et les jetons de bloc dans lesquels des données ont été écrites.

Puis-je obtenir un historique de tous les appels d'API SNS effectués par les API directes EBS sur mon compte à des fins d'analyse de sécurité et de résolution des problèmes opérationnels ?

Oui. Pour recevoir un historique des appels d'API des API directes EBS effectués sur votre compte, activez AWS CloudTrail dans la Console de gestion AWS. Pour de plus amples informations, veuillez consulter [Enregistrez les appels d'API directs EBS à l'aide de AWS CloudTrail](#).

Restaurez les volumes EBS, les instantanés EBS et les EBS-backed AMI supprimés à l'aide de la corbeille

La corbeille est une fonctionnalité de récupération de données qui vous permet de restaurer des volumes EBS, des instantanés EBS et des AMI supprimés accidentellement. EBS-backed Lorsque vous utilisez la corbeille, si vos ressources sont supprimées, elles sont retenues dans la corbeille pendant une période spécifiée avant leur suppression définitive.

Vous pouvez restaurer une ressource à partir de la corbeille à tout moment avant l'expiration de sa période de rétention. Une fois que vous avez restauré une ressource à partir de la corbeille, elle est supprimée de la corbeille et vous pouvez l'utiliser de la même manière que n'importe quelle autre ressource de ce type sur votre compte. Si la période de rétention expire et que la ressource n'est pas restaurée, elle est définitivement supprimée de la corbeille et n'est plus disponible pour restauration.

L'utilisation de la corbeille aide à garantir la continuité métier en protégeant vos données métier critiques contre toute suppression accidentelle.

La corbeille est considérée comme une fonctionnalité de service d'Amazon Elastic Block Store (Amazon EBS). Tous [AWS les services inclus dans le](#) programme de conformité (FedRAMP, HIPAA BAA, SOC, etc.) répertoriant Amazon EBS s'appliqueront également à la corbeille.

Rubriques

- [Ressources prises en charge](#)
- [Comment fonctionne la corbeille ?](#)
- [Considérations concernant la corbeille de recyclage](#)
- [Quotas](#)
- [Services connexes](#)
- [Tarification](#)
- [Contrôlez l'accès à la corbeille avec IAM](#)
- [Création d'une règle de conservation de la corbeille](#)
- [Mettre à jour une règle de conservation des corbeilles existante](#)
- [Verrouiller la règle de conservation d'une corbeille pour empêcher sa mise à jour ou sa suppression](#)

- [Déverrouillez une règle de conservation de la corbeille pour permettre sa mise à jour ou sa suppression](#)
- [Marquer une règle de conservation de la corbeille](#)
- [Supprimer une règle de conservation de la corbeille pour l'empêcher de conserver les ressources](#)
- [Récupérez des instantanés supprimés de la corbeille](#)
- [Récupérez les volumes supprimés de la corbeille](#)
- [Récupérez les AMI supprimées de la corbeille](#)
- [Surveiller la corbeille à l'aide d'Amazon EventBridge](#)
- [Surveillez la corbeille à l'aide AWS CloudTrail](#)
- [Points de terminaison de service pour la corbeille](#)
- [Création d'une connexion privée entre un VPC et la corbeille](#)

Ressources prises en charge

La corbeille prend en charge les types de ressources suivants :

- Volumes Amazon EBS
- Instantanés Amazon EBS

Important

Les règles de conservation de la corbeille s'appliquent également aux instantanés archivés dans le niveau de stockage des archives. Si vous supprimez un instantané archivé qui correspond à une règle de conservation, cet instantané est conservé dans la corbeille pendant la période définie dans la règle de conservation. Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille.

- Images de machines EBS-backed Amazon Amazon (AMI)

Note

Les règles de conservation s'appliquent également aux AMI désactivées.

Comment fonctionne la corbeille ?

Pour activer et utiliser la corbeille, vous devez créer des règles de conservation dans les AWS régions dans lesquelles vous souhaitez protéger vos ressources. Les règles de rétention précisent :

- Type de ressource que vous souhaitez protéger (volumes, instantanés ou AMI).
- Type de règle de conservation :
 - Tag-level règles de conservation : ces règles de conservation utilisent des balises de ressources pour identifier les ressources à protéger. Pour chaque règle de rétention, vous spécifiez une ou plusieurs paires clé-valeur d'identification. Les ressources (du type spécifié) qui possèdent au moins l'une de ces paires clé-valeur de balise sont automatiquement conservées dans la corbeille lors de leur suppression. Utilisez ce type de règle de conservation pour protéger des ressources spécifiques de votre compte en fonction de leurs balises.
 - Region-level règles de conservation : ces règles de conservation s'appliquent par défaut à toutes les ressources (du type spécifié) de la Région, même si les ressources ne sont pas balisées. Vous pouvez toutefois spécifier des balises d'exclusion pour exclure les ressources qui possèdent des balises spécifiques. Utilisez ce type de règle de rétention pour protéger toutes les ressources d'un type spécifique dans une région.
- La période de conservation des ressources après leur suppression. À l'expiration de cette période, les ressources sont définitivement supprimées de la corbeille. Les périodes de conservation prises en charge sont les suivantes :
 - Volumes EBS : 1 à 7 jours
 - Instantanés et EBS-backed AMI EBS : 1 à 365 jours

Lorsqu'une ressource se trouve dans la corbeille, il est possible de la restaurer à tout moment. La ressource reste dans la corbeille jusqu'à ce que l'un des événements suivants se produise :

- Vous le restaurez manuellement pour l'utiliser. Lorsque vous restaurez une ressource à partir de la corbeille, celle-ci est supprimée de la corbeille et elle devient immédiatement disponible pour être utilisée. Vous pouvez utiliser les ressources restaurées de la même manière que n'importe quelle autre ressource de ce type dans votre compte.
- La période de rétention expire. Si la période de rétention expire et que la ressource n'a pas été restaurée à partir de la corbeille, elle est définitivement supprimée de la corbeille et ne peut plus être affichée ou restaurée.

Considérations concernant la corbeille de recyclage

Les points suivants s'appliquent lors de l'utilisation de la corbeille et des règles de rétention.

Considérations d'ordre général

- Les ressources supprimées sont déplacées vers la corbeille uniquement si elles correspondent à une règle de conservation existante. Si vous supprimez une ressource qui ne correspond pas à une règle de rétention, ou si vous n'avez aucune règle de rétention à ce moment-là, cette ressource est définitivement supprimée ; elle n'est pas déplacée vers la corbeille.
-  **Important**

Les règles de rétention suivent un modèle de cohérence éventuel pour la première règle de rétention créée par type de ressource et par région de votre compte. Lorsque vous créez votre première règle de rétention pour un type de ressource dans une région, cette règle peut ne pas être active et commencer à conserver les ressources immédiatement. Cependant, toutes les règles de conservation que vous créez ultérieurement pour ce même type de ressource dans la même région deviendront actives et commenceront à conserver les ressources presque immédiatement.
- Si une ressource correspond à plus d'une règle de conservation lors de la suppression, la règle de conservation ayant la période de conservation la plus longue a la priorité.
- Vous ne pouvez pas supprimer manuellement une ressource de la corbeille. La ressource sera supprimée automatiquement à l'expiration de sa période de rétention.
- Lorsqu'une ressource se trouve dans la corbeille, vous pouvez uniquement l'afficher, la restaurer ou modifier ses identifications. Pour utiliser la ressource d'une autre manière, vous devez d'abord la restaurer.
- Si un outil Service AWS, tel que AWS Backup ou Amazon Data Lifecycle Manager, supprime une ressource qui correspond à une règle de rétention, cette ressource est automatiquement conservée par la corbeille. Si nécessaire, vous pouvez empêcher ces ressources d'entrer dans la corbeille lors de leur suppression en les étiquetant, puis en les ajoutant en tant que balises d'exclusion à vos règles de conservation.
- Lorsqu'une ressource est envoyée à la corbeille, l'identification de génération système suivante est affectée à la ressource :
 - Clé d'identification : `aws:recycle-bin:resource-in-bin`
 - Valeur d'identification : `true`

Vous ne pouvez pas modifier ou supprimer manuellement cette identification. Lorsque la ressource est restaurée à partir de la corbeille, l'identification est automatiquement supprimée.

Considérations relatives aux volumes

- Les volumes supprimés en raison de la fermeture de l'instance ou du remplacement du volume racine sont protégés par la corbeille.
- Les volumes qui ne peuvent pas être créés ne sont pas protégés par la corbeille lors de leur suppression.
- Les volumes de lancements d'instances ayant échoué ne sont pas protégés par la corbeille lors de la suppression.
- Les volumes d'instances gérées ne sont pas protégés par la corbeille lors de leur suppression.
- La création ou la modification de volumes en cours ne seront pas interrompues lorsque le volume entrera dans la corbeille. Cela signifie que vous êtes toujours facturé en conséquence si le volume a été créé avec un tarif provisionné Amazon EBS pour l'initialisation du volume.
- Les volumes placés dans la corbeille sont pris en compte dans vos quotas de la même manière que les volumes normaux.
- Les volumes placés dans la corbeille ne sont pas facturés une fois le délai de sortie de la corbeille écoulé. Vous ne pouvez pas restaurer ces volumes, mais vous pouvez les découvrir s'ils n'ont pas encore été supprimés.
- L'`DeleteVolume` événement ne sera envoyé qu'une fois le volume supprimé de la corbeille. Cet événement n'est pas émis lorsque le volume entre dans la corbeille.

Considérations relatives aux instantanés

-  **Important**
Si vous disposez de règles de rétention pour les AMI et pour leurs instantanés associés, faites en sorte que la période de rétention des instantanés soit identique ou plus longue que la période de rétention des AMI. Cela garantit que la corbeille ne supprime pas les instantanés associés à une AMI avant de supprimer l'AMI elle-même, car cela rendrait l'AMI irrécupérable.
- Si la restauration rapide d'instantané est activée pour un instantané lorsqu'il est supprimé, elle est automatiquement désactivée peu de temps après l'envoi de l'instantané dans la corbeille.

- Si vous restaurez l'instantané avant que la restauration rapide d'instantané ne soit désactivée pour l'instantané, elle reste activée.
- Si vous restaurez l'instantané, une fois que la restauration d'instantané rapide a été désactivée, elle reste désactivée. Si nécessaire, vous devez réactiver manuellement la restauration rapide d'instantané.
- Si un instantané est partagé lors de sa suppression, le partage est automatiquement annulé lorsqu'il est envoyé à la corbeille. Si vous restaurez l'instantané, toutes les autorisations de partage précédentes sont automatiquement restaurées.
- Si un instantané créé par un autre AWS service, par exemple, AWS Backup est envoyé à la corbeille et que vous restaurez ultérieurement cet instantané à partir de la Corbeille, il n'est plus géré par le AWS service qui l'a créé. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Considérations relatives aux AMI

- Seules les EBS-backed AMI Amazon sont prises en charge.

-

Important

Si vous disposez de règles de rétention pour les AMI et pour leurs instantanés associés, faites en sorte que la période de rétention des instantanés soit identique ou plus longue que la période de rétention des AMI. Cela garantit que la corbeille ne supprime pas les instantanés associés à une AMI avant de supprimer l'AMI elle-même, car cela rendrait l'AMI irrécupérable.

- Si une AMI est partagée lors de sa suppression, le partage est automatiquement annulé lorsqu'elle est envoyée à la corbeille. Si vous restaurez l'AMI, toutes les autorisations de partage précédentes sont automatiquement restaurées.
- Avant de pouvoir restaurer une AMI depuis la corbeille, vous devez d'abord restaurer tous ses instantanés associés depuis la Corbeille et vous assurer qu'ils sont en bon available état.
- Si les instantanés associés à l'AMI sont supprimés de la corbeille, l'AMI n'est plus récupérable. L'AMI sera supprimée à l'expiration de la période de rétention.
- Si une AMI créée par un autre AWS service, tel que AWS Backup, est envoyée dans la corbeille et que vous restaurez ultérieurement cette AMI à partir de la Corbeille, elle n'est plus gérée par le AWS service qui l'a créée. Vous devez supprimer manuellement l'AMI si elle n'est plus nécessaire.

Considérations relatives aux politiques d'instantanés Amazon Data Lifecycle Manager

- Si Amazon Data Lifecycle Manager supprime un instantané qui correspond à une règle de conservation, cet instantané est automatiquement conservé par la corbeille.
- Si Amazon Data Lifecycle Manager supprime un instantané et l'envoie à la corbeille lorsque le seuil de rétention de la politique est atteint, et que vous restaurez manuellement l'instantané à partir de la corbeille, vous devez supprimer manuellement cet instantané s'il n'est plus nécessaire. Amazon Data Lifecycle Manager ne gèrera plus l'instantané.
- Si vous supprimez manuellement un instantané créé par une politique et que cet instantané se trouve dans la corbeille lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager ne supprime pas l'instantané. Amazon Data Lifecycle Manager ne gère pas les instantanés lorsqu'ils sont stockés dans la corbeille.

Si l'instantané est restauré à partir de la corbeille avant que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager supprime l'instantané lorsque le seuil de rétention de la politique est atteint.

Si l'instantané est restauré à partir de la corbeille après que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager ne supprime plus l'instantané. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Considérations pour AWS Sauvegarde

- Si AWS Backup supprime un instantané qui correspond à une règle de conservation, cet instantané est automatiquement conservé par la corbeille.

Considérations relatives aux instantanés archivés

- Les règles de conservation de la corbeille s'appliquent également aux instantanés archivés dans le niveau de stockage des archives. Si vous supprimez un instantané archivé qui correspond à une règle de conservation, cet instantané est conservé dans la corbeille pendant la période définie dans la règle de conservation.

Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille.

Si une règle de conservation supprime un instantané archivé de la corbeille avant la période d'archivage minimale de 90 jours, vous êtes facturé pour les jours restants. Pour plus d'informations, consultez la section Tarification et facturation des [instantanés archivés](#).

Pour utiliser un instantané archivé qui se trouve dans la corbeille, vous devez d'abord récupérer l'instantané depuis la corbeille, puis le restaurer du niveau d'archivage au niveau standard.

Quotas

Les quotas suivants s'appliquent à la corbeille.

Quota	Quota par défaut			
Règles de rétention par région	250			
Paires clé-valeur d'identification par règle de rétention	50			

Services connexes

La corbeille fonctionne avec les services suivants :

- AWS CloudTrail : permet d'enregistrer les événements qui se produisent dans la corbeille. Pour de plus amples informations, veuillez consulter [Surveillez la corbeille à l'aide AWS CloudTrail](#).

Tarification

Il n'y a pas de facturation supplémentaire pour l'utilisation de la corbeille et des règles de rétention. Pour plus d'informations, consultez la section [Tarification d'Amazon EBS](#).

- Volumes Amazon EBS : les volumes stockés dans la corbeille sont facturés au même tarif que les volumes réguliers de votre compte.
- Instantanés Amazon EBS : les instantanés enregistrés dans la corbeille sont facturés au même tarif que les instantanés enregistrés normalement sur votre compte.
- EBS-backed AMI — Les AMI stockées dans la corbeille n'entraînent aucun frais supplémentaire.

Note

Certaines ressources peuvent encore apparaître dans la console de la corbeille ou dans la sortie de l'API AWS CLI et pendant une courte période après l'expiration de leur période de conservation et leur suppression définitive. Ces ressources ne vous sont pas facturées. La facturation s'arrête dès que la période de rétention expire.

Vous pouvez utiliser les balises de répartition des coûts AWS générées ci-dessous à des fins de suivi et de répartition des coûts lors de l'utilisation AWS Billing and Cost Management.

- Clé : `aws:recycle-bin:resource-in-bin`
- Valeur : `true`

Pour plus d'informations, veuillez consulter la section [Balises de répartition des coûts générées par AWS](#) dans le Guide de l'utilisateur AWS Billing and Cost Management .

Contrôlez l'accès à la corbeille avec IAM

Par défaut, les utilisateurs ne sont pas autorisés à utiliser la corbeille, les règles de rétention ou les ressources contenues dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Rubriques

- [Autorisations pour utiliser la corbeille et les règles de rétention](#)
- [Autorisations pour utiliser des ressources dans la corbeille](#)
- [Clés de condition pour la corbeille](#)

Autorisations pour utiliser la corbeille et les règles de rétention

Pour utiliser la corbeille et les règles de rétention, les utilisateurs ont besoin des autorisations suivantes.

- `rbn:CreateRule`
- `rbn:UpdateRule`
- `rbn:GetRule`
- `rbn:ListRules`
- `rbn>DeleteRule`
- `rbn:TagResource`
- `rbn:UntagResource`
- `rbn:ListTagsForResource`
- `rbn:LockRule`
- `rbn:UnlockRule`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `tag:GetResources`.

Voici un exemple de politique IAM qui inclut l'autorisation `tag:GetResources` pour les utilisateurs de la console. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rbn:CreateRule",
        "rbn:UpdateRule",
        "rbn:GetRule",
        "rbn:ListRules",
        "rbn>DeleteRule",
        "rbn:TagResource",
```

```

        "rbin:UntagResource",
        "rbin:ListTagsForResource",
        "rbin:LockRule",
        "rbin:UnlockRule",
        "tag:GetResources"
    ],
    "Resource": "*"
}
]
}

```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Autorisations pour utiliser des ressources dans la corbeille

Pour plus d'informations sur les autorisations IAM nécessaires pour travailler avec les ressources de la corbeille, reportez-vous aux rubriques suivantes :

- [Autorisations pour travailler avec des volumes dans la corbeille](#)
- [Autorisations pour utiliser des instantanés dans la corbeille](#)
- [Autorisations pour utiliser des AMI dans la corbeille](#)

Clés de condition pour la corbeille

La corbeille définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM pour contrôler les conditions d'application de l'instruction de stratégie. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

Rubriques

- [rbin : clé de Request/ResourceType condition](#)
- [rbin : clé de Attribute/ResourceType condition](#)

rbin : clé de Request/ResourceType condition

La clé de `rbin:Request/ResourceType` condition peut être utilisée pour filtrer l'accès [CreateRule](#) et les [ListRules](#) demandes en fonction de la valeur spécifiée pour le paramètre de `ResourceType` demande.

Exemple 1 - CreateRule

L'exemple de politique IAM suivant permet aux responsables IAM d'effectuer des `CreateRule` demandes uniquement si la valeur spécifiée pour le paramètre de `ResourceType` demande est `EBS_SNAPSHOT` ou `EC2_IMAGE`. Cela permet au principal de créer de nouvelles règles de rétention pour les instantanés et les AML uniquement.

JSON

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rbin:CreateRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
        }
      }
    }
  ]
}
```

```

    }
  }
]
}

```

Exemple 2 - ListRules

L'exemple de politique IAM suivant permet aux responsables IAM de faire des `ListRules` demandes uniquement si la valeur spécifiée pour le paramètre de `ResourceType` demande est. `EBS_SNAPSHOT` Cela permet au principal de répertorier les règles de rétention pour les instantanés uniquement, et cela les empêche de répertorier les règles de rétention pour tout autre type de ressource.

JSON

```

{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rbin:ListRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
        }
      }
    }
  ]
}

```

rbin : clé de **Attribute/ResourceType** condition

La clé de `rbin:Attribute/ResourceType` condition peut être utilisée pour filtrer l'accès sur [DeleteRule](#), [GetRule](#), [UpdateRule](#), [LockRule](#), [UnlockRule](#), [TagResource](#), [UntagResource](#), et les [ListTagsForResource](#) demandes en fonction de la valeur de l'`ResourceType` attribut de la règle de rétention.

Exemple 1 - UpdateRule

L'exemple de politique IAM suivant permet aux responsables IAM de faire des UpdateRule demandes uniquement si l'ResourceTypeattribut de la règle de rétention demandée est ou. EBS_SNAPSHOT EC2_IMAGE Cela permet au principal de mettre à jour des règles de rétention pour les instantanés et les AMI uniquement.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rbin:UpdateRule"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "rbin:Attribute/ResourceType": ["EBS_SNAPSHOT", "EC2_IMAGE"]
        }
      }
    }
  ]
}
```

Exemple 2 - DeleteRule

L'exemple de politique IAM suivant permet aux responsables IAM de faire des DeleteRule demandes uniquement si l'ResourceTypeattribut de la règle de rétention demandée est. EBS_SNAPSHOT Cela permet au principal de supprimer des règles de rétention pour les instantanés uniquement.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```



```

    {
      "Effect" : "Allow",
      "Action" : [
        "rbin:DeleteRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
        }
      }
    }
  ]
}

```

Création d'une règle de conservation de la corbeille

Lorsque vous créez une règle de conservation, vous devez spécifier les paramètres obligatoires suivants :

- Type de ressource à protéger (volumes, instantanés ou AMI).
- Type de règle de conservation (au niveau de la balise ou Region-level). Tag-level les règles protègent uniquement les ressources qui possèdent des balises spécifiques. Region-level les règles protègent toutes les ressources de la Région, mais peuvent exclure les ressources qui ont des balises spécifiques.
- La période de conservation des ressources après leur suppression. À l'expiration de cette période, les ressources sont définitivement supprimées de la corbeille. Les périodes de conservation prises en charge sont les suivantes :
 - Volumes EBS : 1 à 7 jours
 - Instantanés et EBS-backed AMI EBS : 1 à 365 jours

Vous pouvez également spécifier un nom de règle et une description de 255 caractères maximum chacun, ainsi que des balises pour vous aider à identifier et à organiser vos règles. Nous vous recommandons de ne pas inclure d'informations personnelles, confidentielles ou sensibles dans le nom, la description ou les balises.

Vous pouvez également éventuellement verrouiller les règles Region-level de conservation lors de la création. Si vous verrouillez une règle de conservation lors de sa création, vous devez également

spécifier le délai de déverrouillage, qui peut aller de 7 à 30 jours. Les règles de conservation restent déverrouillées par défaut, à moins que vous ne les verrouilliez explicitement.

 Note

Les règles de rétention fonctionnent uniquement dans les régions où elles ont été créées. Si vous avez l'intention d'utiliser la corbeille dans d'autres régions, vous devez créer des règles de rétention supplémentaires dans ces régions.

Vous pouvez créer une règle de rétention de corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour créer une règle de rétention au niveau des balises

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention), puis Create retention rule (Créer une règle de rétention).
3. (Facultatif) Pour Retention rule name (Nom de la règle de rétention), saisissez un nom descriptif pour la règle de rétention.
4. (Facultatif) Pour Retention rule description (Description de la règle de rétention), saisissez une brève description pour la règle de rétention.
5. Dans Type de ressource, sélectionnez le type de ressource à protéger par la règle de rétention. La règle de rétention conservera uniquement les ressources de ce type dans la corbeille.
6. Pour Sélectionnez les ressources à conserver, choisissez Conserver les ressources dotées de balises spécifiques.
7. Pour les balises de ressources, entrez la clé de balise et les paires de valeurs à utiliser pour identifier les ressources à conserver dans la corbeille. Seules les ressources du type spécifié qui possèdent au moins l'une des balises spécifiées seront conservées par la règle de rétention.
8. Pour Période de conservation, entrez le nombre de jours pendant lesquels les ressources supprimées doivent être conservées dans la corbeille.
9. Choisissez Create retention rule (Créer une règle de rétention).

Pour créer une règle Region-level de rétention

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention), puis Create retention rule (Créer une règle de rétention).
3. (Facultatif) Pour Retention rule name (Nom de la règle de rétention), saisissez un nom descriptif pour la règle de rétention.
4. (Facultatif) Pour Retention rule description (Description de la règle de rétention), saisissez une brève description pour la règle de rétention.
5. Dans Type de ressource, sélectionnez le type de ressource à protéger par la règle de rétention. La règle de rétention conservera uniquement les ressources de ce type dans la corbeille.
6. Pour Sélectionnez les ressources à conserver, choisissez Conserver toutes les ressources.
7. (Facultatif) Pour exclure des ressources qui possèdent des balises spécifiques, dans la zone Balises d'exclusion, entrez jusqu'à cinq paires clé-valeur de balise à utiliser pour identifier les ressources à exclure. Les ressources qui possèdent l'une de ces balises sont ignorées par la règle de rétention.
8. Pour Période de conservation, entrez le nombre de jours pendant lesquels les ressources supprimées doivent être conservées dans la corbeille.
9. (Facultatif) Pour verrouiller la règle de conservation, dans Rule lock settings (Paramètres de verrouillage des règles), sélectionnez Lock (Verrouiller), puis dans Unlock delay period (Délai de déverrouillage), spécifiez le délai de déverrouillage en jours. Une règle de conservation verrouillée ne peut être ni modifiée ni supprimée. Pour modifier ou supprimer la règle, vous devez d'abord la déverrouiller, puis attendre l'expiration du délai de déverrouillage. Pour de plus amples informations, consultez [Verrouiller la règle de conservation d'une corbeille pour empêcher sa mise à jour ou sa suppression](#).

Pour laisser la règle de conservation déverrouillée, dans Rule lock settings (Paramètres de verrouillage des règles), conservez l'option Unlock (Déverrouiller). Une règle de conservation déverrouillée peut être modifiée ou supprimée à tout moment.

Note

Vous ne pouvez pas verrouiller les règles Region-level de conservation qui comportent des balises d'exclusion.

10. Choisissez Create retention rule (Créer une règle de rétention).

AWS CLI

Pour créer une règle de rétention

Utilisez la commande [create-rule](#) de la AWS CLI . Pour `--retention-period`, spécifiez le nombre de jours de rétention des instantanés supprimés dans la corbeille. Pour `--resource-type`, spécifiez `EBS_VOLUME` pour les volumes, `EBS_SNAPSHOT` pour les instantanés ou `EC2_IMAGE` pour les AMI. Pour créer une règle de rétention au niveau des balises `--resource-tags`, pour, spécifiez les balises à utiliser pour identifier les ressources à conserver. Pour créer une règle de Region-level rétention, omettez `--resource-tags` et spécifiez `--exclude-resource-tags` éventuellement d'exclure les ressources qui possèdent des balises spécifiques. Pour verrouiller une règle de Region-level rétention `--lock-configuration`, incluez et spécifiez le délai de déverrouillage en jours.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_VOLUME|EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value \
--exclude-resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Exemple 1

L'exemple de commande suivant crée une règle de Region-level conservation déverrouillée qui conserve tous les instantanés supprimés pendant plusieurs 7 jours.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

Exemple 2

L'exemple de commande suivant crée une règle de niveau identification qui retient les instantanés supprimés qui sont étiquetés `purpose=production` pendant une période de 7 jours.

```
aws rbin create-rule \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Match snapshots with a specific tag" \  
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Exemple 3

L'exemple de commande suivant crée une règle de Region-level conservation verrouillée qui conserve tous les instantanés supprimés pendant plusieurs 7 jours. La règle de conservation est verrouillée avec un délai de déverrouillage de 7 jours.

```
aws rbin create-rule \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Match all snapshots" \  
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Exemple 4

L'exemple de commande suivant crée une règle de Region-level conservation déverrouillée qui conserve tous les instantanés supprimés, à l'exception des instantanés marqués avec `purpose:testing`, pendant quelques jours. 7

```
aws rbin create-rule \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Match only production snapshots" \  
--exclude-resource-tags ResourceTagKey=purpose,ResourceTagValue=testing
```

Mettre à jour une règle de conservation des corbeilles existante

Vous pouvez mettre à jour la description d'une règle de conservation déverrouillée, ses balises de ressource et sa période de conservation à tout moment après sa création. Vous ne pouvez pas mettre à jour le type de ressource ou le délai de déverrouillage d'une règle de conservation, même si la règle de conservation est déverrouillée.

Vous ne pouvez en aucun cas mettre à jour une règle de conservation verrouillée. Si vous devez modifier une règle de conservation verrouillée, vous devez d'abord la déverrouiller, puis attendre l'expiration du délai de déverrouillage.

Si vous devez modifier le délai de déverrouillage d'une règle de conservation verrouillée, vous devez [déverrouiller la règle de conservation](#), puis attendre l'expiration du délai de déverrouillage actuel. Lorsque le délai de déverrouillage est expiré, vous devez [verrouiller à nouveau la règle de conservation](#) et spécifier le nouveau délai de déverrouillage.

 Note

Nous vous recommandons de ne pas inclure de données d'identification personnelle, confidentielles ou sensibles dans la description de la règle de rétention.

Une fois que vous avez mis à jour une règle de rétention, les modifications s'appliquent uniquement aux nouvelles ressources qu'elle retient. Les modifications n'affectent pas les ressources précédemment envoyées à la corbeille. Par exemple, si vous mettez à jour la période de rétention d'une règle de rétention, seuls les instantanés supprimés après la mise à jour sont retenus pour la nouvelle période de rétention. Les instantanés envoyés à la corbeille avant la mise à jour sont retenus pendant la période de rétention précédente (ancienne).

Vous pouvez mettre à jour une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour mettre à jour une règle de rétention

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de rétention à mettre à jour, puis choisissez Actions, Edit retention rule (Modifier une règle de rétention).
4. Dans la section Rule details (Détails de la règle), mettez à jour Retention rule name (Nom de la règle de rétention) et Retention rule description (Description de la règle de rétention), si nécessaire.
5. Dans la section Rule settings (Paramètres de la règle), mettez à jour Resource type (Type de ressource), Resource tags to match (Identifications de ressource à faire correspondre) et Retention period (Période de rétention), si nécessaire.

6. Dans la section Tags (Identifications), ajoutez ou supprimez des identifications de règles de rétention si nécessaire.
7. Choisissez Save retention rule (Enregistrer la règle de rétention).

AWS CLI

Pour mettre à jour une règle de rétention

Utilisez la commande [update-rule](#) de la AWS CLI . Pour `--identifier`, spécifiez l'ID de la règle de rétention pour laquelle mettre à jour `--resource-types`, spécifiez EBS_VOLUME pour les volumes, EBS_SNAPSHOT pour les instantanés ou EC2_IMAGE pour les AML.

```
aws rbin update-rule \  
--identifier rule_ID \  
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \  
--resource-type EBS_VOLUME|EBS_SNAPSHOT|EC2_IMAGE \  
--description "rule_description"
```

Exemple

L'exemple de commande suivant met à jour la règle de rétention 6lsJ2Fa9nh9 pour retenir tous les instantanés pour 7 jours et met à jour sa description.

```
aws rbin update-rule \  
--identifier 6lsJ2Fa9nh9 \  
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \  
--resource-type EBS_SNAPSHOT \  
--description "Retain for three weeks"
```

Verrouiller la règle de conservation d'une corbeille pour empêcher sa mise à jour ou sa suppression

La corbeille vous permet de verrouiller les règles de Region-level conservation à tout moment.

Une règle de conservation verrouillée ne peut être ni modifiée ni supprimée, même par les utilisateurs disposant des autorisations IAM requises. Verrouillez vos règles de conservation pour les protéger contre les modifications et les suppressions accidentelles ou malveillantes.

Lorsque vous verrouillez une règle de conservation, vous devez spécifier un délai de déverrouillage. Il s'agit de la période de temps que vous devez attendre après avoir déverrouillé la règle de conservation avant de pouvoir la modifier ou la supprimer. Vous ne pouvez ni modifier ni supprimer la règle de conservation pendant le délai de déverrouillage. Vous pouvez modifier ou supprimer la règle de conservation qu'une fois le délai de déverrouillage expiré.

Vous ne pouvez pas modifier la période de déverrouillage après le verrouillage de la règle de conservation. Si les autorisations de votre compte ont été compromises, le délai de déverrouillage vous donne plus de temps pour détecter les menaces de sécurité et y répondre. La durée de cette période doit être plus longue que le temps nécessaire à pour identifier les failles de sécurité et y répondre. Pour définir la durée appropriée, vous pouvez passer en revue les incidents de sécurité précédents et le temps nécessaire pour identifier et corriger une violation de compte.

Nous vous recommandons d'utiliser EventBridge les règles Amazon pour vous informer des modifications de l'état de verrouillage des règles de rétention. Pour de plus amples informations, veuillez consulter [Surveiller la corbeille à l'aide d'Amazon EventBridge](#).

Considérations

- Vous ne pouvez pas verrouiller les règles de rétention au niveau des balises ou les règles de Region-level rétention qui comportent des balises d'exclusion.
- Vous pouvez verrouiller une règle de conservation déverrouillée à tout moment.
- Le délai de déverrouillage doit être de 7 à 30 jours.
- Vous pouvez verrouiller à nouveau une règle de conservation pendant le délai de déverrouillage. Verrouiller à nouveau la règle de conservation réinitialise le délai de déverrouillage.

Vous pouvez verrouiller une règle Region-level de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour verrouiller une règle de conservation

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le panneau de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de conservation déverrouillée que vous souhaitez verrouiller, puis choisissez Actions, Edit retention rule lock (Modifier le verrouillage d'une règle de conservation).

4. Dans l'écran Edit retention rule lock (Modifier le verrouillage d'une règle de conservation), choisissez Lock (Verrouiller), puis pour Unlock delay period (Délai de déverrouillage), spécifiez le délai de déverrouillage en jours.
5. Cochez la case I acknowledge that locking the retention rule will prevent it from being modified or deleted (Je reconnais que le verrouillage de la règle de conservation empêchera sa modification ou sa suppression), puis choisissez Save (Enregistrer).

AWS CLI

Pour verrouiller une règle de conservation déverrouillée

Utilisez la commande AWS CLI [lock-rule](#). Pour `--identifier`, spécifiez l'ID de la règle de conservation à verrouiller. Pour `--lock-configuration`, spécifiez le délai de déverrouillage en jours.

```
aws rbin lock-rule \  
--identifier rule_ID \  
--lock-configuration  
'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Exemple

L'exemple de commande suivant verrouille la règle de conservation 6lsJ2Fa9nh9 et définit le délai de déverrouillage sur 15 jours.

```
aws rbin lock-rule \  
--identifier 6lsJ2Fa9nh9 \  
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Déverrouillez une règle de conservation de la corbeille pour permettre sa mise à jour ou sa suppression

Vous ne pouvez ni modifier ni supprimer une règle de conservation verrouillée. Si vous devez modifier une règle de conservation verrouillée, vous devez d'abord la déverrouiller. Après avoir déverrouillé la règle de conservation, vous devez attendre que le délai de déverrouillage expire avant de pouvoir la modifier ou la supprimer. Vous ne pouvez ni modifier ni supprimer une règle de rétention pendant le délai de déverrouillage.

Une règle de conservation déverrouillée peut être modifiée et supprimée à tout moment par un utilisateur disposant des autorisations IAM requises. Le fait de laisser vos règles de conservation déverrouillées peut les exposer à des modifications et à des suppressions accidentelles ou malveillantes.

Considérations

- Vous pouvez verrouiller à nouveau une règle de conservation pendant le délai de déverrouillage.
- Vous pouvez verrouiller à nouveau une règle de conservation une fois le délai de déverrouillage expiré.
- Vous ne pouvez pas contourner le délai de déverrouillage.
- Vous ne pouvez pas modifier le délai de déverrouillage après le verrouillage initial.

Nous vous recommandons d'utiliser EventBridge les règles Amazon pour vous informer des modifications de l'état de verrouillage des règles de rétention. Pour de plus amples informations, veuillez consulter [Surveiller la corbeille à l'aide d'Amazon EventBridge](#).

Vous pouvez déverrouiller une règle de Region-level rétention verrouillée à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour déverrouiller une règle de conservation

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le panneau de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de conservation verrouillée que vous souhaitez déverrouiller, puis choisissez Actions, Edit retention rule lock (Modifier le verrouillage d'une règle de conservation).
4. Sur l'écran Edit retention rule lock (Modifier le verrouillage d'une règle de conservation), choisissez Unlock (Déverrouiller), puis Save (Enregistrer).

AWS CLI

Pour déverrouiller une règle de conservation verrouillée

Utilisez la commande AWS CLI [unlock-rule](#). Pour `--identifier`, spécifiez l'ID de la règle de conservation à déverrouiller.

```
aws rbin unlock-rule \  
--identifiant rule_ID
```

Exemple

L'exemple de commande suivant déverrouille la règle de conservation 6lsJ2Fa9nh9

```
aws rbin unlock-rule \  
--identifiant 6lsJ2Fa9nh9
```

Marquer une règle de conservation de la corbeille

Vous pouvez affecter des identifications personnalisées à vos règles de rétention pour classer celles-ci de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Cela vous permet de trouver de manière efficace une règle de rétention spécifique en fonction des identifications personnalisées que vous avez affectées.

Vous pouvez affecter une identification à une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour étiqueter une règle de rétention

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention à étiqueter, choisissez l'onglet Tags (Identifications), puis choisissez Manage tags (Gérer les identifications).
4. Choisissez Ajouter une balise. Pour Key (Clé), saisissez la clé de l'identification. Pour Value (Valeur), saisissez la valeur de l'identification.
5. Choisissez Save (Enregistrer).

AWS CLI

Pour étiqueter une règle de rétention

Utilisez la commande [tag-resource](#) AWS CLI . Pour `--resource-arn`, indiquez l'Amazon Resource Name (ARN) de la règle de rétention à étiqueter, et pour `--tags`, spécifiez la paire clé-valeur d'identification.

```
aws rbin tag-resource \  
--resource-arn retention_rule_arn \  
--tags key=tag_key,value=tag_value
```

Exemple

L'exemple de commande suivant étiquette la règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3` avec l'identification `purpose=production`.

```
aws rbin tag-resource \  
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \  
--tags key=purpose,value=production
```

Afficher les identifications de règle de rétention

Vous pouvez afficher les identifications affectées à une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour afficher les identifications d'une règle de rétention

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention pour laquelle afficher les identifications, puis choisissez l'onglet Tags (Identifications).

AWS CLI

Pour afficher les identifications affectées à une règle de rétention

Utilisez la commande [list-tags-for-resource](#) de la AWS CLI . Pour `--resource-arn`, spécifiez l'ARN de la règle de rétention.

```
aws rbin list-tags-for-resource \  

```

```
--resource-arn retention_rule_arn
```

Exemple

L'exemple de commande suivant répertorie les identifications de règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3`.

```
aws rbin list-tags-for-resource \  
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3
```

Supprimer les identifications des règles de rétention

Vous pouvez supprimer les identifications d'une règle de rétention en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour supprimer une identification d'une règle de rétention

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention dont vous souhaitez supprimer une identification et choisissez Tags (Identifications), puis Manage tags (Gérer les identifications).
4. Choisissez Remove (Supprimer) en regard de l'identification à supprimer.
5. Choisissez Save (Enregistrer).

AWS CLI

Pour supprimer une identification d'une règle de rétention

Utilisez la commande [untag-resource](#) de la AWS CLI . Pour `--resource-arn`, spécifiez l'ARN de la règle de rétention. Pour `--tagkeys`, spécifiez les clés d'identifications des identifications à supprimer.

```
aws rbin untag-resource \  
--resource-arn retention_rule_arn \  
--tagkeys tag_key
```

Exemple

Voici un exemple de commande supprimant les identifications disposant d'une clé d'identification de type `purpose` de la règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3`.

```
aws rbin untag-resource \  
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \  
--tagkeys purpose
```

Supprimer une règle de conservation de la corbeille pour l'empêcher de conserver les ressources

Vous pouvez supprimer une règle de rétention à tout moment. Lorsque vous supprimez une règle de rétention, elle ne retient plus les nouvelles ressources dans la corbeille une fois qu'elles ont été supprimées. Les ressources envoyées à la corbeille avant la suppression de la règle de rétention continuent d'être retenues dans la corbeille en fonction de la période de rétention définie dans la règle de rétention. Lorsque la période expire, l'instantané est définitivement supprimé de la corbeille.

Vous pouvez supprimer une règle de rétention en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour supprimer une règle de rétention

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de rétention à supprimer, puis choisissez Actions, Delete retention rule (Supprimer la règle de rétention).
4. Lorsque vous y êtes invité, saisissez le message de confirmation et choisissez Delete retention rule (Supprimer la règle de rétention).

AWS CLI

Pour supprimer une règle de rétention

Utilisez la commande [delete-rule](#) de la AWS CLI . Pour `--identifier`, spécifiez l'ID de la règle de rétention à supprimer.

```
aws rbin delete-rule --identifieur rule_ID
```

Exemple

L'exemple de commande suivant supprime la règle de rétention 61sJ2Fa9nh9.

```
aws rbin delete-rule --identifieur 61sJ2Fa9nh9
```

Récupérez des instantanés supprimés de la corbeille

Cette rubrique explique comment récupérer des instantanés Amazon EBS depuis la corbeille.

Rubriques

- [Autorisations pour utiliser des instantanés dans la corbeille](#)
- [Afficher les instantanés dans la corbeille](#)
- [Restaurer des instantanés à partir de la corbeille](#)

Autorisations pour utiliser des instantanés dans la corbeille

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les instantanés contenus dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Pour afficher et récupérer des instantanés qui se trouvent dans la corbeille, les utilisateurs doivent disposer des autorisations suivantes :

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Pour gérer les identifications des instantanés dans la corbeille, les utilisateurs ont besoin des autorisations supplémentaires suivantes.

- `ec2:CreateTags`
- `ec2>DeleteTags`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `ec2:DescribeTags`.

Voici un exemple de politique IAM. Elle comprend l'autorisation `ec2:DescribeTags` pour les utilisateurs de la console et les autorisations `ec2:CreateTags` et `ec2:DeleteTags` pour la gestion des identifications. Si les autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations nécessaires pour utiliser la corbeille, consultez [Autorisations pour utiliser la corbeille et les règles de rétention](#).

Afficher les instantanés dans la corbeille

Lorsqu'un instantané se trouve dans la corbeille, vous pouvez afficher des informations limitées à son sujet, notamment :

- ID de l'instantané
- la description de l'instantané ;
- l'ID du volume à partir duquel l'instantané a été créé ;
- la date et l'heure de la suppression de l'instantané et de son entrée dans la corbeille ;

- la date et l'heure d'expiration de la période de rétention ; à ce moment-là, l'instantané sera définitivement supprimé de la corbeille.

Vous pouvez afficher les instantanés dans la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour visualiser les instantanés dans la corbeille à l'aide de la console

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les instantanés qui se trouvent actuellement dans la corbeille. Pour afficher les détails d'un instantané spécifique, sélectionnez-le dans la grille et choisissez Actions, View details (Afficher les détails).

AWS CLI

Pour afficher des instantanés dans la corbeille à l'aide du AWS CLI

Utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/list-snapshots-in-recycle-bin.html> AWS CLI `list-snapshots-in-recycle-bin`. Incluez l'option `--snapshot-id` pour afficher un instantané spécifique ou omettez l'option `--snapshot-id` pour afficher tous les instantanés dans la corbeille.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Par exemple, la commande suivante renvoie des informations sur l'instantané `snap-01234567890abcdef` dans la corbeille.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Exemple de sortie :

```
{
  "SnapshotRecycleBinInfo": [
    {
      "Description": "Monthly data backup snapshot",
      "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
```

```
    "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",  
    "VolumeId": "vol-abcdef09876543210",  
    "SnapshotId": "snap-01234567890abcdef"  
  }  
]  
}
```

Restaurer des instantanés à partir de la corbeille

Vous ne pouvez en aucun cas utiliser un instantané lorsqu'il se trouve dans la corbeille. Pour utiliser l'instantané, vous devez d'abord le restaurer. Lorsque vous restaurez un instantané à partir de la corbeille, il est immédiatement disponible pour utilisation et il est supprimé de la corbeille. Une fois qu'il est restauré, vous pouvez l'utiliser de la même manière que n'importe quel autre instantané de votre compte.

Vous pouvez restaurer un instantané à partir de la corbeille en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour restaurer un instantané à partir de la corbeille en utilisant la console

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les instantanés qui se trouvent actuellement dans la corbeille. Sélectionnez l'instantané à restaurer, puis choisissez Recover (Récupérer).
4. Lorsque vous y êtes invité, choisissez Recover (Récupérer).

AWS CLI

Pour restaurer un instantané supprimé de la corbeille à l'aide du AWS CLI

Utilisez la commande [restore-snapshot-from-recycle-bin](#) AWS CLI . Pour `--snapshot-id`, spécifiez l'ID de l'instantané à restaurer.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Par exemple, la commande suivante restaure l'instantané `snap-01234567890abcdef` depuis la corbeille.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Exemple de sortie :

```
{
  "SnapshotId": "snap-01234567890abcdef",
  "Description": "Monthly data backup snapshot",
  "Encrypted": false,
  "OwnerId": "111122223333",
  "Progress": "100%",
  "StartTime": "2021-12-01T13:00:00.000000+00:00",
  "State": "recovering",
  "VolumeId": "vol-ffffffff",
  "VolumeSize": 30
}
```

Récupérez les volumes supprimés de la corbeille

Cette rubrique explique comment récupérer des volumes Amazon EBS depuis la corbeille.

Rubriques

- [Autorisations pour travailler avec des volumes dans la corbeille](#)
- [Afficher les volumes dans la corbeille](#)
- [Restaurer les volumes depuis la corbeille](#)

Autorisations pour travailler avec des volumes dans la corbeille

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les volumes qui se trouvent dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Pour consulter et récupérer les volumes qui se trouvent dans la corbeille, les utilisateurs doivent disposer des autorisations suivantes :

- `ec2:ListVolumesInRecycleBin`

- `ec2:RestoreVolumeFromRecycleBin`

Pour gérer les balises des volumes de la corbeille, les utilisateurs ont besoin des autorisations supplémentaires suivantes.

- `ec2:CreateTags`
- `ec2>DeleteTags`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `ec2:DescribeTags`.

Voici un exemple de politique IAM. Elle comprend l'autorisation `ec2:DescribeTags` pour les utilisateurs de la console et les autorisations `ec2:CreateTags` et `ec2>DeleteTags` pour la gestion des identifications. Si les autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRecycleBinVolumeOperations",
      "Effect": "Allow",
      "Action": [
        "ec2:ListVolumesInRecycleBin",
        "ec2:RestoreVolumeFromRecycleBin"
      ],
      "Resource": "arn:aws:ec2:*:123456789012:volume/*"
    },
    {
      "Sid": "AllowVolumeTagOperations",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:DescribeTags"
      ],
      "Resource": "arn:aws:ec2:*:123456789012:volume/*"
    }
  ]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations nécessaires pour utiliser la corbeille, consultez [Autorisations pour utiliser la corbeille et les règles de rétention](#).

Afficher les volumes dans la corbeille

Lorsqu'un volume se trouve dans la corbeille, vous pouvez consulter des informations limitées à son sujet, notamment :

- ID du volume.
- Taille du volume.
- Type de volume.
- Date et heure auxquelles le volume a été supprimé et est entré dans la corbeille.
- la date et l'heure d'expiration de la période de rétention ; Le volume sera définitivement supprimé de la corbeille à ce stade.

Vous pouvez consulter les volumes de la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour afficher les volumes dans la corbeille à l'aide de la console

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les volumes qui se trouvent actuellement dans la corbeille. Pour afficher les détails d'un volume spécifique, sélectionnez-le dans la grille et choisissez Actions, Afficher les détails.

AWS CLI

Pour afficher les volumes dans la corbeille à l'aide du AWS CLI

Utilisez la commande [list-volumes-in-recycle-bin](#) AWS CLI . Incluez l'`--volume-idoption` permettant d'afficher un volume spécifique. Ou omettez l'`--volume-idoption` permettant d'afficher tous les volumes de la corbeille.

```
aws ec2 list-volumes-in-recycle-bin --volume-id volume_id
```

Par exemple, la commande suivante fournit des informations sur le volume `vol-01234567890abcdef` de la corbeille.

```
aws ec2 list-volumes-in-recycle-bin --volume-id vol-01234567890abcdef
```

Exemple de sortie :

```
{
  "VolumeRecycleBinInfo": [
    {
      "VolumeId": "vol-01234567890abcdef",
      "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
      "RecycleBinExitTime": "2021-12-08T13:00:00.000Z"
    }
  ]
}
```

Restaurer les volumes depuis la corbeille

Vous ne pouvez en aucun cas utiliser un volume lorsqu'il se trouve dans la corbeille. Pour utiliser le volume, vous devez d'abord le restaurer. Lorsque vous restaurez un volume depuis la corbeille, le volume est immédiatement disponible pour utilisation et il est supprimé de la Corbeille. Vous pouvez utiliser un volume restauré de la même manière que n'importe quel autre volume de votre compte.

Vous pouvez restaurer un volume depuis la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour restaurer un volume depuis la corbeille à l'aide de la console

1. Ouvrez la console de la corbeille à l'adresse <https://console.aws.amazon.com/rbin/home/>
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les volumes qui se trouvent actuellement dans la corbeille. Sélectionnez le volume à restaurer et choisissez Restaurer.
4. Lorsque vous y êtes invité, choisissez Recover (Récupérer).

AWS CLI

Pour restaurer un volume supprimé de la corbeille à l'aide du AWS CLI

Utilisez la commande [restore-volume-from-recycle-bin](#) AWS CLI . Pour `--volume-id`, spécifiez l'ID du volume à restaurer.

```
aws ec2 restore-volume-from-recycle-bin --volume-id volume_id
```

Par exemple, la commande suivante restaure le volume `vol-01234567890abcdef` depuis la corbeille.

```
aws ec2 restore-volume-from-recycle-bin --volume-id vol-01234567890abcdef
```

Exemple de sortie :

```
{
  "VolumeId": "vol-01234567890abcdef",
  "State": "available",
  "Size": 100,
```

```
"VolumeType": "gp3",  
"AvailabilityZone": "us-east-1a",  
"CreateTime": "2021-12-01T13:00:00.000000+00:00",  
"Encrypted": false  
}
```

Récupérez les AMI supprimées de la corbeille

Cette rubrique explique comment récupérer des EBS-backed AMI Amazon depuis la corbeille.

Rubriques

- [Autorisations pour utiliser des AMI dans la corbeille](#)
- [Afficher les AMI dans la corbeille](#)
- [Restaurer des AMI depuis la corbeille](#)

Autorisations pour utiliser des AMI dans la corbeille

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les AMI contenues dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Pour afficher et récupérer des AMI qui se trouvent dans la corbeille, les utilisateurs doivent disposer des autorisations suivantes :

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

Pour gérer les identifications des AMI dans la corbeille, les utilisateurs ont besoin des autorisations supplémentaires suivantes.

- `ec2:CreateTags`
- `ec2>DeleteTags`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `ec2:DescribeTags`.

Voici un exemple de politique IAM. Elle comprend l'autorisation `ec2:DescribeTags` pour les utilisateurs de la console et les autorisations `ec2:CreateTags` et `ec2:DeleteTags` pour la gestion des identifications. Si les autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique [Création d'un jeu d'autorisations](#) du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations nécessaires pour utiliser la corbeille, consultez [Autorisations pour utiliser la corbeille et les règles de rétention](#).

Afficher les AMI dans la corbeille

Lorsqu'une AMI se trouve dans la corbeille, vous pouvez afficher des informations limitées à son sujet, notamment :

- Le nom, la description et l'ID unique de l'AMI.
- La date et l'heure de la suppression de l'AMI et de son entrée dans la corbeille.
- la date et l'heure d'expiration de la période de rétention ; L'AMI sera définitivement supprimée à ce moment-là.

Vous pouvez afficher les AMI dans la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour visualiser les AMI supprimées dans la corbeille à l'aide de la console

1. Ouvrez la console de la corbeille à l'adresse console.aws.amazon.com/rbin/accueil/.
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie toutes les ressources qui se trouvent actuellement dans la corbeille. Pour afficher les détails d'une AMI spécifique, sélectionnez-la dans la grille et choisissez Actions, View details (Afficher les détails).

AWS CLI

Pour afficher les AMI supprimées dans la corbeille à l'aide du AWS CLI

Utilisez la commande [list-images-in-recycle-bin](#) AWS CLI . Pour afficher des AMI spécifiques, incluez l'option `--image-id` et spécifiez les ID des AMI à afficher. Vous pouvez spécifier jusqu'à 20 ID dans une seule demande.

Pour afficher toutes les AMI de la corbeille, omettez l'option `--image-id`. Si vous ne spécifiez pas de valeur pour `--max-items`, la commande renvoie par défaut 1 000 éléments par page. Pour plus d'informations, consultez [Pagination](#) dans le manuel Amazon EC2 API Reference.

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Par exemple, la commande suivante renvoie des informations sur l'AMI `ami-01234567890abcdef` dans la corbeille.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Exemple de sortie :

```
{
  "Images": [
    {
      "ImageId": "ami-0f740206c743d75df",
      "Name": "My AL2 AMI",
      "Description": "My Amazon Linux 2 AMI",
      "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
      "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
```

```
}  
]  
}
```

Important

Si le message d'erreur suivant s'affiche, il se peut que vous deviez mettre à jour votre AWS CLI version. Pour plus d'informations, veuillez consulter la rubrique [Erreurs liées aux commandes introuvables](#).

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Restaurer des AMI depuis la corbeille

Vous ne pouvez en aucun cas utiliser une AMI lorsqu'elle se trouve dans la corbeille. Pour utiliser l'AMI, vous devez d'abord la restaurer. Lorsque vous restaurez une AMI à partir de la corbeille, elle est immédiatement disponible pour utilisation et elle est supprimée de la corbeille. Une fois qu'elle est restaurée, vous pouvez l'utiliser de la même manière que n'importe quelle autre AMI de votre compte.

Vous pouvez restaurer une AMI à partir de la corbeille en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour restaurer une AMI depuis la corbeille en utilisant la console

1. Ouvrez la console de la corbeille à l'adresse console.aws.amazon.com/rbin/accueil/.
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie toutes les ressources qui se trouvent actuellement dans la corbeille. Sélectionnez l'AMI à restaurer, puis choisissez Recover (Récupérer).
4. Lorsque vous y êtes invité, choisissez Recover (Récupérer).

AWS CLI

Pour restaurer une AMI supprimée de la corbeille à l'aide du AWS CLI

Utilisez la commande [restore-image-from-recycle-bin](#) AWS CLI . Pour `--image-id`, spécifiez l'ID de l'AMI à restaurer.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Par exemple, la commande suivante restaure l'AMI `ami-01234567890abcdef` depuis la corbeille.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

La commande ne renvoie aucun résultat en cas de succès.

Important

Si le message d'erreur suivant s'affiche, il se peut que vous deviez mettre à jour votre AWS CLI version. Pour plus d'informations, veuillez consulter la rubrique [Erreurs liées aux commandes introuvables](#).

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Surveiller la corbeille à l'aide d'Amazon EventBridge

La corbeille envoie des événements à Amazon EventBridge pour les actions effectuées sur les règles de conservation. Avec EventBridge, vous pouvez établir des règles qui déclenchent des actions programmatiques en réponse à ces événements. Par exemple, vous pouvez créer une EventBridge règle qui envoie une notification par e-mail lorsqu'une règle de rétention est déverrouillée et qu'elle entre dans son délai de déverrouillage. Pour plus d'informations, consultez [Création de EventBridge règles Amazon qui réagissent aux événements](#).

Les événements dans EventBridge sont représentés sous forme d'objets JSON. Les champs spécifiques à l'événement figurent dans la section `detail` de l'objet JSON. Le champ `event` contient le nom de l'événement. Le champ `result` contient l'état terminé de l'action qui lance l'événement. Pour plus d'informations, consultez les modèles EventBridge d'événements [Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations sur Amazon EventBridge, consultez [Qu'est-ce qu'Amazon EventBridge ?](#) dans le guide de EventBridge l'utilisateur Amazon.

Événements

- [RuleLocked](#)

- [RuleChangeAttempted](#)
- [RuleUnlockScheduled](#)
- [RuleUnlockingNotice](#)
- [RuleUnlocked](#)

RuleLocked

Voici un exemple d'événement généré par la corbeille lorsqu'une règle de conservation est correctement verrouillée. Cet événement peut être généré par `CreateRule` et par des `LockRule` demandes. L'API qui a généré l'événement est indiquée dans le champ `api-name`.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Locked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail": {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "CreateRule"
  }
}
```

RuleChangeAttempted

Voici un exemple d'événement généré par la corbeille lors de tentatives infructueuses de modification ou de suppression d'une règle verrouillée. Cet événement peut être généré par `DeleteRule` et par des `UpdateRule` demandes. L'API qui a généré l'événement est indiquée dans le champ `api-name`.

```
{
  "version": "0",
```

```

{id": "exampleb-b491-4cf7-a9f1-bf370example",
"detail-type": "Recycle Bin Rule Change Attempted",
"source": "aws.rbin",
"account": "123456789012",
"time": "2022-08-10T16:37:50Z",
"region": "us-west-2",
"resources": [
"arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
],
"detail":
{
"detail-version": " 1.0.0",
"rule-id": "a12345abcde",
"rule-description": "locked account level rule",
"unlock-delay-period": "30 days",
"api-name": "DeleteRule"
}
}

```

RuleUnlockScheduled

Voici un exemple d'événement généré par la corbeille lorsqu'une règle de conservation est déverrouillée et qu'elle commence son délai de déverrouillage.

```

{
"version": "0",
"id": "exampleb-b491-4cf7-a9f1-bf370example",
"detail-type": "Recycle Bin Rule Unlock Scheduled",
"source": "aws.rbin",
"account": "123456789012",
"time": "2022-08-10T16:37:50Z",
"region": "us-west-2",
"resources": [
"arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
],
"detail":
{
"detail-version": " 1.0.0",
"rule-id": "a12345abcde",
"rule-description": "locked account level rule",
"unlock-delay-period": "30 days",
"scheduled-unlock-time": "2022-09-10T16:37:50Z",
}
}

```

```
}
```

RuleUnlockingNotice

Voici un exemple d'événement généré quotidiennement par la corbeille alors qu'une règle de conservation est dans son délai de déverrouillage, jusqu'à la veille de l'expiration du délai de déverrouillage.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocking Notice",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail": {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

RuleUnlocked

Voici un exemple d'événement généré par la corbeille lorsque le délai de déverrouillage d'une règle de conservation expire et que la règle de rétention peut être modifiée ou supprimée.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
```

```
"region": "us-west-2",
"resources": [
  "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
],
"detail": {
  "detail-version": " 1.0.0",
  "rule-id": "a12345abcde",
  "rule-description": "locked account level rule",
  "unlock-delay-period": "30 days",
  "scheduled-unlock-time": "2022-09-10T16:37:50Z"
}
```

Surveillez la corbeille à l'aide AWS CloudTrail

Le service Recycle Bin est intégré à AWS CloudTrail. CloudTrail est un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture tous les appels d'API effectués dans la corbeille sous forme d'événements. Si vous créez un historique, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon Simple Storage Service (Amazon S3). Si vous ne configurez pas de journal, vous pouvez toujours consulter les événements de gestion les plus récents sur la CloudTrail console dans l'historique des événements. Vous pouvez utiliser les informations collectées CloudTrail pour déterminer la demande qui a été faite à la corbeille, l'adresse IP à partir de laquelle la demande a été faite, qui l'a faite, quand elle a été faite et des informations supplémentaires.

Pour plus d'informations à ce sujet CloudTrail, consultez le Guide de [AWS CloudTrail l'utilisateur](#).

Informations sur la corbeille dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité liée à un événement pris en charge se produit dans la corbeille, cette activité est enregistrée dans un CloudTrail événement avec les autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents sur votre AWS compte. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#).

Pour un enregistrement permanent des événements de votre AWS compte, y compris les événements relatifs à la corbeille, créez un historique. Un trail permet CloudTrail de transmettre des

fichiers journaux à un bucket S3. Par défaut, lorsque vous créez un historique dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en profondeur les données d'événements collectées dans les CloudTrail journaux et y donner suite. Pour plus d'informations, consultez la section [Overview for creating a trail](#) dans le Guide de l'utilisateur AWS CloudTrail .

Actions d'API prises en charge

Pour la corbeille, vous pouvez CloudTrail enregistrer les actions d'API suivantes en tant qu'événements de gestion.

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

Pour plus d'informations sur la gestion de la journalisation des événements, consultez la section [Journalisation des événements de gestion des sentiers](#) dans le Guide de CloudTrail l'utilisateur.

Informations relatives à l'identité

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré 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 effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.

- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'[CloudTrail utilisateur IdentityElement](#).

Comprendre les entrées du fichier journal de la corbeille

Un journal est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne sont pas une pile ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Voici des exemples d'entrées de CloudTrail journal.

CreateRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-08-02T21:43:38Z"
    }
  },
  "eventTime": "2021-08-02T21:45:22Z",
  "eventSource": "rbin.amazonaws.com",
```

```

"eventName": "CreateRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 boto/1.21.9",
"requestParameters": {
  "retentionPeriod": {
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  },
  "description": "Match all snapshots",
  "resourceType": "EBS_SNAPSHOT"
},
"responseElements": {
  "identifier": "jkrnexample"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

GetRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",

```

```

    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
},
{
  "eventTime": "2021-08-02T21:45:33Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}

```

ListRules

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",

```

```

"principalId": "123456789012",
"arn": "arn:aws:iam::123456789012:root",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
},
"eventTime": "2021-08-02T21:44:37Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "ListRules",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 boto3/1.21.9",
"requestParameters": {
"resourceTags": [
  {
    "resourceTagKey": "test",
    "resourceTagValue": "test"
  }
]
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",

```

```

"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

UpdateRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-08-02T21:43:38Z"
    }
  },
  "eventTime": "2021-08-02T21:46:03Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 boto3/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample",
    "retentionPeriod": {
      "retentionPeriodValue": 365,
      "retentionPeriodUnit": "DAYS"
    }
  },

```

```

"description": "Match all snapshots",
"resourceType": "EBS_SNAPSHOT"
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

DeleteRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
},

```

```

"eventTime": "2021-08-02T21:46:25Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "DeleteRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
  "identifier": "jkrnexample"
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

TagResource

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      }
    }
  },

```



```

    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-10-22T21:38:34Z"
    }
  },
  "eventTime": "2021-10-22T21:43:15Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 boto3/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tags": [
      {
        "key": "purpose",
        "value": "production"
      }
    ]
  },
  "responseElements": null,
  "requestID": "examplee-7962-49ec-8633-795efexample",
  "eventID": "example4-6826-4c0a-bdec-0bab1example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}

```

UntagResource

```

{
  "eventVersion": "1.08",
  "userIdentity": {

```

```

"type": "AssumedRole",
"principalId": "123456789012",
"arn": "arn:aws:iam::123456789012:root",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-10-22T21:38:34Z"
  }
},
"eventTime": "2021-10-22T21:44:16Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UntagResource",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
"requestParameters": {
"resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
"tagKeys": [
  "purpose"
]
},
"responseElements": null,
"requestID": "example7-6c1e-4f09-9e46-bb957example",
"eventID": "example6-75ff-4c94-a1cd-4d5f5example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",

```

```
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

ListTagsForResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-10-22T21:38:34Z"
    }
  },
  "eventTime": "2021-10-22T21:42:31Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListTagsForResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
  },
  "responseElements": null,
  "requestID": "example8-10c7-43d4-b147-3d9d9example",
  "eventID": "example2-24fc-4da7-a479-c9748example",
  "readOnly": true,
```

```

"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

LockRule

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:45:19Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "LockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {

```

```

"identifiant": "jkrnexample",
"lockConfiguration": {
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
},
},
"responseElements": {
  "identifiant": "jkrnexample",
  "description": "",
  "resourceType": "EBS_SNAPSHOT",
  "retentionPeriod": {
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  },
  "resourceTags": [],
  "status": "available",
  "lockConfiguration": {
    "unlockDelay": {
      "unlockDelayValue": 7,
      "unlockDelayUnit": "DAYS"
    }
  },
  "lockState": "locked"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}

```

UnlockRule

```
{
```

```
"eventVersion": "1.08",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "123456789012",
  "arn": "arn:aws:iam::123456789012:root",
  "accountId": "123456789012",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "123456789012",
      "arn": "arn:aws:iam::123456789012:role/Admin",
      "accountId": "123456789012",
      "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2022-10-25T00:45:11Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2022-10-25T00:46:17Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UnlockRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "python-requests/2.25.1",
"requestParameters": {
  "identifier": "jkrnexample"
},
"responseElements": {
  "identifier": "jkrnexample",
  "description": "",
  "resourceType": "EC2_IMAGE",
  "retentionPeriod": {
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  }
},
"resourceTags": [],
"status": "available",
"lockConfiguration": {
  "unlockDelay": {
    "unlockDelayValue": 7,
```

```
    "unlockDelayUnit": "DAYS"
  },
  "lockState": "pending_unlock",
  "lockEndTime": "Nov 1, 2022, 12:46:17 AM"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

Points de terminaison de service pour la corbeille

Un point de terminaison est une URL qui sert de point d'entrée à un service AWS Web. La corbeille prend en charge les types de terminaux suivants :

- Points de terminaison IPv4
- Dual-stack terminaux prenant en charge à la fois IPv4 et IPv6
- Points de terminaison FIPS

Lorsque vous faites une demande, vous pouvez spécifier le point de terminaison et la région à utiliser. Si vous ne spécifiez pas de point de terminaison, le point de terminaison IPv4 est utilisé par défaut. Pour utiliser un autre type de point de terminaison, vous devez le spécifier dans votre demande. Pour obtenir un exemple de la façon de procéder, consultez [Spécification des points de terminaison](#).

Pour la corbeille, voir les points de terminaison de la [corbeille](#) dans le Référence générale d'Amazon Web Services.

Rubriques

- [Points de terminaison IPv4](#)
- [Dual-stack terminaux \(IPv4 et IPv6\)](#)
- [Points de terminaison FIPS](#)
- [Spécification des points de terminaison](#)

Points de terminaison IPv4

Les points de terminaison IPv4 prennent en charge le trafic IPv4 uniquement. Les points de terminaison IPv4 sont disponibles pour toutes les régions.

Vous devez spécifier la région dans le nom du point de terminaison. Les noms des points de terminaison utilisent la convention de dénomination suivante :

- `poubelle.region.amazonaws.com`

Par exemple, le point de terminaison IPv4 pour la région USA Est (Virginie du Nord) est `estrbn.us-east-1.amazonaws.com`.

Dual-stack terminaux (IPv4 et IPv6)

Dual-stack les terminaux prennent en charge le trafic IPv4 et IPv6. Dual-stack les points de terminaison sont disponibles pour toutes les régions.

Pour utiliser IPv6, vous devez utiliser un point de terminaison à double pile. Lorsque vous adressez une requête à un point de terminaison à double pile, l'URL du point de terminaison se résout en une adresse IPv6 ou IPv4, selon le protocole utilisé par votre réseau et votre client.

Vous devez spécifier la région dans le nom du point de terminaison. Dual-stack les noms de points de terminaison utilisent la convention de dénomination suivante :

- `rbn.region.api.aws`

Par exemple, le point de terminaison à double pile pour la région de l'Est des États-Unis (Virginie du Nord) est `estrbn.us-east-1.api.aws`.

Points de terminaison FIPS

La corbeille fournit des points de terminaison FIPS-validated IPv4 et à double pile (IPv4 et IPv6) pour les régions suivantes :

- `us-east-1` : USA Est (Virginie du Nord)
- `us-east-2` : USA Est (Ohio)
- `us-west-1` : USA Ouest (Californie du Nord)
- `us-west-2` : USA Ouest (Oregon)
- `ca-central-1` : Canada (Centre)
- `ca-west-1` — Canada-Ouest (Calgary)
- `us-gov-east-1` — AWS GovCloud (US-East)
- `us-gov-west-1` — AWS GovCloud (US-West)

Les points de terminaison IPv4 FIPS utilisent la convention d'affectation de noms suivante : `rbin-fips.region.amazonaws.com`. Par exemple, le point de terminaison IPv4 FIPS pour la région de l'Est des États-Unis (Virginie du Nord) est `rbin-fips.us-east-1.amazonaws.com`

Les points de terminaison FIPS à double pile utilisent la convention d'affectation de noms suivante : `rbin-fips.region.api.aws`. Par exemple, le point de terminaison FIPS à double pile pour la région de l'Est des États-Unis (Virginie du Nord) est `rbin-fips.us-east-1.api.aws`

Spécification des points de terminaison

Les exemples suivants montrent comment spécifier un point de terminaison pour la région `us-east-2` à l'aide de AWS CLI.

- Dual-stack

```
aws rbin get-rule \  
--identifiant rule_id \  
--endpoint-url https://rbin.us-east-2.api.aws
```

- IPv4

```
aws rbin get-rule \  
--identifiant rule_id \  

```

```
--endpoint-url https://rbin.us-east-2.amazonaws.com
```

Création d'une connexion privée entre un VPC et la corbeille

Vous pouvez établir une connexion privée entre votre VPC et la corbeille en créant une interface VPC endpoint, alimentée par [AWS PrivateLink](#). Vous pouvez accéder à la corbeille comme si elle se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou de Direct Connect connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec la corbeille.

Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface.

Pour plus d'informations, consultez la section [Accès aux AWS services AWS PrivateLink](#) dans le AWS PrivateLink Guide.

Créer un point de terminaison VPC d'interface pour la corbeille

Vous pouvez créer un point de terminaison VPC pour la corbeille à l'aide de la console Amazon VPC ou du AWS CLI. Pour plus d'informations, consultez [Créer un point de terminaison d'un VPC](#) dans le Guide AWS PrivateLink.

Créez un point de terminaison VPC pour la corbeille en utilisant le nom de service suivant : `com.amazonaws.region.rb`

Si vous activez le DNS privé pour le terminal, vous pouvez envoyer des requêtes d'API à la corbeille en utilisant son nom DNS par défaut pour la région, par exemple `rb.in.us-east-1.amazonaws.com`.

Création d'une politique de point de terminaison VPC pour la corbeille

Par défaut, l'accès complet à la corbeille est autorisé via le terminal. Vous pouvez contrôler l'accès au point de terminaison de l'interface à l'aide des politiques de point de terminaison VPC. Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès à la corbeille. La politique spécifie les informations suivantes :

- Le `principal` qui peut effectuer des actions.
- Les `actions` qui peuvent être effectuées.

- Les ressources sur lesquelles les actions peuvent être effectuées.

Pour de plus amples informations, veuillez consulter [Contrôle de l'accès aux services avec points de terminaison d'un VPC](#) dans le Amazon VPC Guide de l'utilisateur.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "rbin:*",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Effect": "Deny",
      "Action": "rbin:DeleteRule",
      "Resource": "*",
      "Principal": "*",
      "Condition": {
        "StringEquals" : {
          "rbin:Attribute/ResourceType": "EBS_SNAPSHOT"
        }
      }
    }
  ]
}
```

Sécurité dans Amazon EBS

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- **Sécurité du cloud** : AWS est chargée de protéger l'infrastructure qui exécute les AWS 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 Programmes](#) de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Elastic Block Store, consultez la section [AWS Services concernés par programme de conformitéAWS](#) .
- **Sécurité dans le cloud** — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon EBS. Les rubriques suivantes expliquent comment configurer Amazon EBS pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Amazon EBS.

Rubriques

- [Protection des données dans Amazon EBS](#)
- [Gestion des identités et des accès pour Amazon EBS](#)
- [Validation de conformité pour Amazon EBS](#)
- [Résilience des données dans Amazon EBS](#)

Protection des données dans Amazon EBS

Le modèle de responsabilité AWS <https://aws.amazon.com/compliance/shared-responsibility-model/> s'applique à la protection des données dans Amazon Elastic Block Store. Comme décrit dans ce

modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère tous les 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 Amazon EBS ou autre à Services AWS l'aide de la console, de l'API ou des 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.

Rubriques

- [Sécurité des données Amazon EBS](#)
- [Chiffrement au repos et en transit](#)
- [Gestion des clés KMS](#)

Sécurité des données Amazon EBS

Les volumes Amazon EBS vous sont présentés comme des périphériques de stockage en mode bloc bruts non formatés. Ces périphériques sont des périphériques logiques créés sur l'infrastructure EBS. Le service Amazon EBS garantit que les appareils sont logiquement vides (c'est-à-dire que les blocs bruts sont mis à zéro ou contiennent des données cryptographiquement pseudo-aléatoires) avant toute utilisation ou réutilisation par le client.

Si vos procédures nécessitent l'effacement de toutes les données à l'aide d'une méthode spécifique, telle que celles détaillées dans le DoD 5220.22-M (National Industrial Security Program Operating Manual) ou le NIST 800-88 (Directives pour la désinfection des supports), vous pouvez le faire sur Amazon EBS. Vous pouvez effacer les données avant ou après utilisation, ou les deux selon les exigences de la procédure. Cette activité de niveau bloc sera reflétée sur le support de stockage sous-jacent du service Amazon EBS.

Chiffrement au repos et en transit

Le chiffrement Amazon EBS est une solution de chiffrement qui vous permet de chiffrer vos volumes Amazon EBS et vos instantanés Amazon EBS à l'aide de clés cryptographiques. AWS Key Management Service Les opérations de chiffrement EBS ont lieu sur les serveurs qui hébergent les instances Amazon EC2. Cela garantit la sécurité des données au repos et des données en transit entre une instance et son volume attaché, ainsi que tous les instantanés ultérieurs. Pour de plus amples informations, veuillez consulter [Chiffrement Amazon EBS](#).

Gestion des clés KMS

Lorsque vous créez un volume ou un instantané Amazon EBS chiffré, vous spécifiez une AWS Key Management Service clé. Par défaut, Amazon EBS utilise la clé KMS AWS gérée pour Amazon EBS dans votre compte et votre région (aws/ebs). Vous pouvez toutefois spécifier une clé KMS gérée

par le client que vous créez et gérez. L'utilisation d'une clé KMS gérée par le client vous offre plus de flexibilité, notamment la possibilité de créer, de modifier et de désactiver des clés KMS.

Pour utiliser une clé KMS gérée par le client, vous devez autoriser les utilisateurs à utiliser la clé KMS. Pour de plus amples informations, veuillez consulter [Autorisations pour les utilisateurs](#).

 Important

Amazon EBS prend uniquement en charge les clés KMS [symétriques](#). Vous ne pouvez pas utiliser de clés KMS [asymétriques](#) pour chiffrer un volume et des instantanés Amazon EBS. Pour savoir si une clé KMS est symétrique ou asymétrique, voir [Identifier les clés KMS asymétriques](#).

Pour chaque volume, Amazon EBS demande de AWS KMS générer une clé de données unique chiffrée selon la clé KMS que vous spécifiez. Amazon EBS stocke la clé de données chiffrée avec le volume. Ensuite, lorsque vous attachez le volume à une instance Amazon EC2, Amazon EBS appelle AWS KMS pour déchiffrer la clé de données. Amazon EBS utilise la clé de données en texte brut de la mémoire de l'hyperviseur pour chiffrer le tout I/O sur le volume. Pour de plus amples informations, veuillez consulter [Comment fonctionne le chiffrement Amazon EBS](#).

Gestion des identités et des accès pour Amazon EBS

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 les ressources Amazon EBS. 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 EBS fonctionne avec IAM](#)
- [Exemples de politiques IAM pour Amazon EBS](#)
- [Résoudre les problèmes d'autorisation Amazon EBS](#)

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'autorisation Amazon EBS](#))
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir [Comment Amazon EBS fonctionne avec IAM](#))
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir [Exemples de politiques IAM pour Amazon EBS](#))

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 EBS fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon EBS, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Amazon EBS.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Elastic Block Store

Fonctionnalité IAM	Assistance Amazon EBS
Identity-based politiques	Oui
Resource-based politiques	Non

Fonctionnalité IAM	Assistance Amazon EBS
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Service-linked rôles	Non

Pour obtenir une vue d'ensemble de la façon dont Amazon EBS et d'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 Amazon EBS

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 Amazon EBS

Pour consulter des exemples de politiques basées sur l'identité Amazon EBS, consultez. [Exemples de politiques IAM pour Amazon EBS](#)

Resource-based politiques au sein d'Amazon EBS

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 stratégiques pour Amazon EBS

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 actions Amazon EBS, consultez [Actions, ressources et clés de condition pour Amazon EC2](#) et [Actions, ressources et clés de condition pour Amazon EBS](#) dans la référence d'autorisation de service.

Les actions de stratégie dans Amazon EBS utilisent soit le préfixe `ec2` soit le `ebs` préfixe situé avant l'action.

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [  
  "ec2:action1",  
  "ec2:action2"  
]
```

Pour consulter des exemples de politiques basées sur l'identité Amazon EBS, consultez. [Exemples de politiques IAM pour Amazon EBS](#)

Ressources relatives aux politiques pour Amazon EBS

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": "*"
```

Certaines actions de l'API Amazon EBS prennent en charge plusieurs ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules. Par exemple, `DescribeVolumes` accède aux `vol-01234567890abcdef` et `vol-09876543210fedcba`. Un principal doit donc être autorisé à accéder aux deux ressources.

```
"Resource": [  
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-01234567890abcdef",  
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-09876543210fedcba"  
]
```

Clés de condition de politique pour Amazon EBS

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.

Par exemple, la condition suivante permet au principal d'effectuer une action sur un volume uniquement si le type de volume est `gp2`.

```
"Condition":{
  "StringLikeIfExists":{
    "ec2:VolumeType":"gp2"
  }
}
```

Pour consulter la liste des clés de condition Amazon EBS, consultez la section [Actions, ressources et clés de condition](#) dans la référence d'autorisation de service.

ACL dans Amazon EBS

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 Amazon EBS

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 attacher 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.

Utilisation d'informations d'identification temporaires avec Amazon EBS

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.

Cross-service autorisations principales pour Amazon EBS

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 Amazon EBS

Prend en charge les rôles de service : oui

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 interrompre les fonctionnalités d'Amazon EBS. Modifiez les rôles de service uniquement lorsque Amazon EBS vous fournit des instructions à cet effet.

Service-linked rôles pour Amazon EBS

Prend en charge les rôles liés à un service : non

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.

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.

Exemples de politiques IAM pour Amazon EBS

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon EBS. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API Console de gestion AWS, AWS Command Line Interface (AWS CLI) ou de AWS l'API. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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 dans l'onglet JSON](#) dans le Guide de l'utilisateur IAM.

Rubriques

- [Bonnes pratiques en matière de politiques](#)

- [Autoriser les utilisateurs à utiliser la console Amazon EBS](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)
- [Autoriser les utilisateurs à travailler avec des volumes](#)
- [Autoriser les utilisateurs à travailler avec des instantanés](#)

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer des ressources Amazon EBS sur votre compte, y accéder ou les 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.

Autoriser les utilisateurs à utiliser la console Amazon EBS

Pour accéder à la console Amazon Elastic Block Store, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations sur les ressources Amazon EBS de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour vous assurer que les utilisateurs et les rôles peuvent toujours utiliser la console Amazon EBS, associez également la politique Amazon EBS *ConsoleAccess* ou *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez [Ajout d'autorisations à un utilisateur](#) 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 des autorisations 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": "*"
  }
]
}

```

Autoriser les utilisateurs à travailler avec des volumes

Exemples

- [Exemple : Attacher et détacher des volumes](#)
- [Exemple : Créer un volume](#)
- [Exemple : Créer un volume avec des balises](#)
- [Exemple : utilisation de volumes à l'aide de la console Amazon EC2](#)

Exemple : Attacher et détacher des volumes

Quand une action d'API requiert qu'un principal spécifie plusieurs ressources, vous devez créer une déclaration de politique qui permet aux utilisateurs d'accéder à toutes les ressources requises. Si vous devez utiliser un élément `Condition` avec une ou plusieurs de ces ressources, vous devez créer plusieurs déclarations, comme dans l'exemple ci-dessous.

La stratégie suivante permet aux utilisateurs d'attacher des volumes avec la balise `"volume_user=nom-utilisateur-iam"` aux instances avec la balise `"department=dev"`, et de détacher ces volumes de ces instances. Si vous attachez cette politique à un groupe IAM, la variable de politique `aws:username` accorde à chaque utilisateur du groupe l'autorisation d'attacher des volumes aux instances (ou de les en détacher) avec une balise nommée `volume_user` qui a son nom d'utilisateur comme valeur.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "StringEquals": {
```

```

    "aws:ResourceTag/volume_user": "${aws:username}"
  }
}
]
}

```

Exemple : Créer un volume

La politique suivante permet aux utilisateurs d'utiliser l'action d'[CreateVolume](#) API. L'utilisateur est autorisé à créer un volume uniquement si le volume est chiffré et seulement si la taille du volume est inférieure à 20 Gio.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "NumericLessThan": {
          "ec2:VolumeSize": "20"
        },
        "Bool": {
          "ec2:Encrypted": "true"
        }
      }
    }
  ]
}

```

Exemple : Créer un volume avec des balises

La stratégie suivante inclut la clé de condition `aws:RequestTag` qui exige aux utilisateurs d'attribuer des balises aux volumes qu'ils créent avec les balises `costcenter=115` et `stack=prod`. Si les

utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

Pour les actions de création de ressources qui appliquent des balises, les utilisateurs doivent être autorisés à effectuer l'action `CreateTags`. La deuxième déclaration utilise la clé de condition `ec2:CreateAction` pour permettre aux utilisateurs de créer des balises uniquement dans le contexte de `CreateVolume`. Les utilisateurs ne peuvent pas attribuer des balises à des volumes existants ou à d'autres ressources.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCreateTaggedVolumes",
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateVolume"
        }
      }
    }
  ]
}
```

La politique suivante permet aux utilisateurs de créer un volume sans avoir à spécifier des balises. L'action `CreateTags` est uniquement évaluée si les balises sont spécifiées dans la demande `CreateVolume`. Si les utilisateurs spécifient une balise, elle doit être `purpose=test`. Aucune autre balise n'est autorisée dans la demande.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/purpose": "test",
          "ec2:CreateAction": "CreateVolume"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "purpose"
        }
      }
    }
  ]
}
```

Exemple : utilisation de volumes à l'aide de la console Amazon EC2

La politique suivante autorise les utilisateurs à afficher et à créer des volumes, ainsi qu'à associer et détacher des volumes à des instances spécifiques à l'aide de la console Amazon EC2.

Les utilisateurs peuvent attacher un volume aux instances ayant la balise `purpose=test`, ainsi que détacher des volumes de ces instances. Pour attacher un volume à l'aide de la console Amazon

EC2, il est utile que les utilisateurs aient l'autorisation d'utiliser l'action `ec2:DescribeInstances`, car ils peuvent ainsi sélectionner une instance dans la liste préremplie de la boîte de dialogue Attacher un volume. Cependant, comme cela permet aussi aux utilisateurs d'afficher toutes les instances sur la page Instances de la console, vous pouvez ignorer cette action.

Dans la première instruction, l'`ec2:DescribeAvailabilityZones` action est nécessaire pour s'assurer qu'un utilisateur peut sélectionner une zone de disponibilité lors de la création d'un volume.

Les utilisateurs ne peuvent pas baliser les volumes qu'ils créent (pendant ou après la création de volume).

Autoriser les utilisateurs à travailler avec des instantanés

Cette section contient des exemples de stratégie pour `CreateSnapshot` (instantané à un instant donné d'un volume EBS) et `CreateSnapshots` (instantanés multi-volumes).

Exemples

- [Exemple : Créer un instantané](#)
- [Exemple : Créer des instantanés](#)
- [Exemple : Créer un instantané avec des balises](#)
- [Exemple : Créer des instantanés multi-volumes avec des identifications](#)
- [Exemple : Copier des instantanés](#)
- [Exemple : Modifier les paramètres d'autorisation d'instantanés](#)

Exemple : Créer un instantané

La politique suivante permet aux clients d'utiliser l'action d'[CreateSnapshot](#) API. Le client peut créer des instantanés uniquement si le volume est chiffré et seulement si la taille du volume est inférieure à 20 Gio.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
```

```

        "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
    },
    {
        "Effect": "Allow",
        "Action": "ec2:CreateSnapshot",
        "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "Condition": {
            "NumericLessThan": {
                "ec2:VolumeSize": "20"
            },
            "Bool": {
                "ec2:Encrypted": "true"
            }
        }
    }
]
}

```

Exemple : Créer des instantanés

La politique suivante permet aux clients d'utiliser l'action d'[CreateSnapshots](#) API. Le client peut créer des instantanés seulement si tous les volumes sur l'instance sont de type GP2.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": [
                "arn:aws:ec2:us-east-1::snapshot/*",
                "arn:aws:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": "arn:aws:ec2:us-east-1:*:volume/*",
            "Condition": {
                "StringLikeIfExists": {

```

```

        "ec2:VolumeType": "gp2"
      }
    }
  ]
}

```

Exemple : Créer un instantané avec des balises

La stratégie suivante inclut la clé de condition `aws:RequestTag`, qui nécessite que le client applique les balises `costcenter=115` et `stack=prod` à tout nouvel instantané. Si les utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

Pour les actions de création de ressources qui appliquent des balises, les clients doivent être autorisés à effectuer l'action `CreateTags`. La troisième déclaration utilise la clé de condition `ec2:CreateAction` pour permettre aux clients de créer des balises uniquement dans le contexte de `CreateSnapshot`. Les clients ne peuvent pas attribuer des balises à des volumes existants ou à d'autres ressources.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*"
    },
    {
      "Sid": "AllowCreateTaggedSnapshots",
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
      }
    }
  ]
}

```

```

        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction": "CreateSnapshot"
        }
      }
    }
  ]
}

```

Exemple : Créer des instantanés multi-volumes avec des identifications

La politique suivante comprend la clé de condition `aws:RequestTag` qui exige que le client applique les identifications `costcenter=115` et `stack=prod` lors de la création d'un jeu d'instantanés multi-volumes. Si les utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": [
        "arn:aws:ec2:us-east-1::snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid": "AllowCreateTaggedSnapshots",
      "Effect": "Allow",

```

```

    "Action": "ec2:CreateSnapshots",
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/costcenter": "115",
            "aws:RequestTag/stack": "prod"
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": "CreateSnapshots"
            }
        }
    }
]
}

```

La politique suivante permet aux clients de créer un instantané sans avoir à spécifier des balises. L'action `CreateTags` est évaluée uniquement si des balises sont spécifiées dans la demande `CreateSnapshot` ou `CreateSnapshots`. Les identifications peuvent être omises dans la demande. Si une balise est spécifiée, elle doit être de type `purpose=test`. Aucune autre balise n'est autorisée dans la demande.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",

```

```

    "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/purpose": "test",
        "ec2:CreateAction": "CreateSnapshot"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": "purpose"
      }
    }
  }
]
}

```

La politique suivante permet aux clients de créer des jeux d'instantanés multi-volumes sans avoir à spécifier des identifications. L'action `CreateTags` est évaluée uniquement si des balises sont spécifiées dans la demande `CreateSnapshot` ou `CreateSnapshots`. Les identifications peuvent être omises dans la demande. Si une balise est spécifiée, elle doit être de type `purpose=test`. Aucune autre balise n'est autorisée dans la demande.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/purpose": "test",
          "ec2:CreateAction": "CreateSnapshots"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": "purpose"
        }
      }
    }
  ]
}

```

```

    }
  }
}
]
}

```

La stratégie suivante permet de créer des instantanés uniquement si le volume source est balisé avec `User:username` pour le client et que l'instantané lui-même est balisé avec `Environment:Dev` et `User:username`. Le client peut ajouter des balises supplémentaires à l'instantané.

La stratégie suivante pour `CreateSnapshots` permet de créer des instantanés uniquement si le volume source est balisé avec `User:username` pour le client et que l'instantané lui-même est balisé avec `Environment:Dev` et `User:username`.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1:*:instance/*"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/User": "${aws:username}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshots",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {

```

```

        "aws:RequestTag/Environment": "Dev",
        "aws:RequestTag/User": "${aws:username}"
    }
},
{
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
}
]
}

```

La stratégie suivante permet de supprimer un instantané uniquement s'il est balisé à l'aide de User:username pour le client.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/User": "${aws:username}"
                }
            }
        }
    ]
}

```

La stratégie suivante permet à un client de créer un instantané mais l'empêche d'exécuter cette action si l'instantané créé comporte une clé de balise value=stack.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": "stack"
        }
      }
    }
  ]
}
```

La stratégie suivante permet à un client de créer des instantanés mais l'empêche d'exécuter cette action si les instantanés créés comportent une clé de balise `value=stack`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshots",
        "ec2:CreateTags"
      ],

```

```

        "Resource": "*"
    },
    {
        "Effect": "Deny",
        "Action": "ec2:CreateSnapshots",
        "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": "stack"
            }
        }
    }
]
}

```

La politique suivante vous permet d'associer plusieurs actions dans une même politique. Vous pouvez uniquement créer un instantané (dans le contexte de `CreateSnapshots`) lorsque l'instantané est créé dans la région `us-east-1`. Vous pouvez uniquement créer des instantanés (dans le contexte de `CreateSnapshots`) lorsque les instantanés sont créés dans la région `us-east-1` et que le type d'instance est `t2*`.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots",
                "ec2:CreateSnapshot",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "ec2:Region": "us-east-1"
                }
            }
        }
    ]
}

```

```

    },
    "StringLikeIfExists": {
      "ec2:InstanceType": ["t2.*"]
    }
  }
}
]
}

```

Exemple : Copier des instantanés

Resource-level les autorisations spécifiées pour l'CopySnapshotaction s'appliquent à la fois au nouvel instantané et à l'instantané source.

L'exemple de stratégie suivant permet aux principaux de copier des instantanés uniquement si le nouvel instantané est créé avec la clé de balise purpose et la valeur de balise production (purpose=production).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCopySnapshotWithTags",
      "Effect": "Allow",
      "Action": "ec2:CopySnapshot",
      "Resource": "arn:aws:ec2:*:111122223333:snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/purpose": "production"
        }
      }
    }
  ]
}

```

L'exemple de politique suivant permet aux administrateurs de copier des instantanés uniquement si l'instantané source appartient AWS au compte. 123456789012

L'exemple de politique suivant permet aux administrateurs de copier des instantanés uniquement si l'instantané source est créé avec la clé de balise de. CSISnapshotName

```
{
  "Effect": "Allow",
  "Action": "ec2:CopySnapshot",
  "Resource": "arn:aws:ec2:*::snapshot/${*}",
  "Condition": {
    "StringLike": {
      "aws:RequestTag/CSISnapshotName": "*"
    }
  }
},

{
  "Effect": "Allow",
  "Action": "ec2:CopySnapshot",
  "Resource": "arn:aws:ec2:*::snapshot/snap-*"
}
```

Exemple : Modifier les paramètres d'autorisation d'instantanés

La politique suivante autorise la modification d'un instantané uniquement si celui-ci est balisé avec `User: username`, où se *username* trouve le nom d'utilisateur du AWS compte du client. La demande échoue si cette condition n'est pas respectée.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifySnapshotAttribute",
      "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/user-name": "${aws:username}"
        }
      }
    }
  ]
}
```

}

Résoudre les problèmes d'autorisation Amazon EBS

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon EBS et IAM.

Problèmes

- [Je ne suis pas autorisé à effectuer une action dans Amazon EBS](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite autoriser des personnes extérieures à mon Compte AWS pour accéder à mes ressources Amazon EBS](#)

Je ne suis pas autorisé à effectuer une action dans Amazon EBS

Si cela vous Console de gestion AWS indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur mateojackson IAM essaie d'utiliser la console pour afficher les détails d'un volume mais ne `ec2:DescribeVolumes` dispose pas d'autorisations.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:DescribeVolumes on resource: volume-id
```

Dans ce cas, Mateo demande à son AWS administrateur de l'autoriser à décrire le volume.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole` action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon EBS.

Certains vos 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 effectuer une action dans Amazon EBS. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle 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 ressources Amazon EBS

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 Amazon EBS prend en charge ces fonctionnalités, consultez [Comment Amazon EBS fonctionne 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.

Validation de conformité pour Amazon EBS

Notre nouvelle expérience AWS d'inscription n'est pas conçue pour les charges de travail réglementées. Si vous utilisez notre nouvelle interface d' AWS inscription, mais que vous souhaitez l'utiliser AWS pour des charges de travail réglementées, vous pouvez vous [inscrire à des fonctionnalités AWS \(avancées\)](#) ou [activer des fonctionnalités avancées](#) pour votre AWS environnement.

Pour savoir si un s' Service AWS inscrit dans le cadre de programmes de conformité spécifiques, consultez [Services AWS la section Étendue par programme de conformité](#) et choisissez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes](#) .

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 la section AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez [AWS la documentation de sécurité](#).

Résilience des données dans Amazon EBS

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, 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 à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Outre l'infrastructure AWS mondiale, Amazon EBS propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

- Automatisation des instantanés EBS à l'aide d'Amazon Data Lifecycle Manager
- Copie des instantanés EBS entre régions

Outils de surveillance pour Amazon EBS

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Elastic Block Store et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Amazon EBS, signaler un problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrail capture les appels d'API et les événements associés effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Les API permettant de gérer vos volumes et vos instantanés EBS font partie de l'API Amazon EC2. Pour plus d'informations sur CloudTrail l'API Amazon EC2, consultez la section [Enregistrer les appels d'API Amazon EC2 à AWS CloudTrail l'aide du guide](#) de l'utilisateur Amazon EC2.
- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour de plus amples informations, veuillez consulter [the section called "Amazon CloudWatch"](#).
- Amazon EventBridge peut être utilisé pour automatiser vos AWS services et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour de plus amples informations, veuillez consulter [the section called "Amazon EventBridge"](#).
- Les statistiques de performances détaillées d'Amazon EBS fournissent des statistiques de I/O performance en temps réel pour les volumes Amazon EBS attachés aux instances Amazon Nitro-based EC2. Pour plus d'informations, consultez [Statistiques de performances détaillées d'Amazon EBS](#).
- Amazon GuardDuty aide à détecter les activités potentiellement malveillantes dans vos instances EC2. GuardDuty Malware Protection for EC2 analyse les volumes EBS attachés à vos instances EC2. Pour de plus amples informations, veuillez consulter [the section called "Amazon GuardDuty"](#).

Statistiques CloudWatch Amazon pour Amazon EBS

Les CloudWatch métriques Amazon sont des données statistiques que vous pouvez utiliser pour visualiser, analyser et configurer des alarmes sur le comportement opérationnel de vos volumes.

Les données sont disponibles automatiquement toutes les minutes sans coût aucun.

Lorsque vous obtenez des données de CloudWatch, vous pouvez inclure un paramètre de `Period` demande pour spécifier la granularité des données renvoyées. Cette période est différente de celle utilisée par EBS pour collecter les données (périodes d'une minute). Nous vous recommandons de spécifier dans votre demande une période égale ou supérieure à la période de collecte afin de vous assurer que les données renvoyées sont valides.

Vous pouvez obtenir les données à l'aide de l' CloudWatch API ou de la console Amazon EC2. La console prend les données brutes de l' CloudWatch API et affiche une série de graphiques basés sur les données. En fonction de vos besoins, vous pouvez préférez utiliser les données de l'API ou les graphiques de la console.

Rubriques

- [Métriques pour les volumes Amazon EBS](#)
- [Statistiques pour les instantanés Amazon EBS](#)
- [Métriques d'instances Nitro](#)
- [Métriques de restauration d'instantané rapide](#)
- [Graphiques de la console Amazon EC2](#)

Métriques pour les volumes Amazon EBS

L'espace de noms AWS/EBS inclut les métriques suivantes pour les volumes EBS attachés à tous les types d'instance. Tous les types de volumes Amazon EBS envoient automatiquement des métriques d'une minute à une CloudWatch instance, mais uniquement lorsque le volume est attaché à une instance.

Pour obtenir des informations sur l'espace disque disponible à partir du système d'exploitation sur une instance, consultez [Afficher l'espace disque disponible](#).

Note

Certaines de ces métriques présentent des différences par rapport aux instances conçues sur le système Nitro. Pour obtenir la liste de ces types d'[instances](#), consultez [Instances basées sur le système Nitro](#).

Métrique	Description	Unités	Dimensions	Statistiques significatives
----------	-------------	--------	------------	-----------------------------

VolumeAvg
IOPS *

Note

Pris en charge pour tous les types de volumes EBS associés aux instances Nitro. Non publié pour les volumes associés à Amazon ECS et AWS Fargate les tâches.

Ops/s

VolumeId
|
InstanceId

- Sum
- Average
- Minimum
- Maximum

Le nombre moyen d'IOPS en lecture et en écriture transmis au volume en une minute. Si aucune opération n'a été portée au volume au cours de la dernière minute, la valeur de la métrique est zéro (0). Pour de plus amples

Métrique	Description	Unités	Dimensions	Statistiques significatives
----------	-------------	--------	------------	-----------------------------

informations, veuillez consulter [Surveillez les I/O caractéristiques à l'aide CloudWatch](#).

Pour les volumes Multi-Attach activés, utilisez la InstanceId dimension pour afficher la moyenne des IOPS pour un attachement d'instance de volume spécifique.

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeAvgThroughput *	<div>  Note Pris en charge pour tous les types de volumes EBS associés aux instances Nitro. Non publié pour les volumes associés à Amazon ECS et AWS Fargate les tâches. </div> <p>Débit moyen de lecture et d'écriture transmis au volume en une minute. Si aucune opération n'a été portée au volume au cours de la dernière minute, la valeur de la métrique est zéro (0). Pour de plus amples informations, veuillez consulter Surveillez les I/O caractéristiques à l'aide CloudWatch.</p> <p>Pour les volumes Multi-Attach activés, utilisez la</p>	KiB/s	VolumeId InstanceId	<ul style="list-style-type: none"> • Sum • Average • Minimum Maximum

Métrique	Description	Unités	Dimensions	Statistiques significatives
	InstanceId dimension pour afficher le débit moyen pour une pièce jointe à une instance de volume spécifique.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeAvgReadLatency *	<div><div><div>Note</div><div>Pris en charge pour tous les types de volumes associés aux instances Nitro. Non publié pour les volumes associés à Amazon ECS et AWS Fargate les tâches.</div></div></div>	Millisecondes	VolumeId InstanceId	Minimum Maximum
<div><div></div><div>Temps moyen nécessaire pour terminer les opérations de lecture en une minute. Utilisez cette métrique pour surveiller la I/O latence moyenne des volumes EBS attachés à vos instances Amazon EC2. La moyenne est calculée sur la base I/O des opérations effectuées au cours de la dernière minute. Si aucune opération n'a été effectuée au cours de la</div></div>				

Métrique	Description	Unités	Dimensions	Statistiques significatives
	dernière minute, la valeur de la métrique est zéro.			
	Pour les volumes Multi-Attach activés, utilisez la InstanceId dimension pour afficher la latence moyenne pour un attachement d'instance de volume spécifique.			

Métrique	Description	Uunités	Dimension s	Statistiq ues significa tives
VolumeAvg WriteLate ncy *	<div><div><div><div><div><div></div><div>Note</div></div></div><div><div>Pris en charge pour tous les types de volumes associés aux instances Nitro. Non publié pour les volumes associés à Amazon ECS et AWS Fargate les tâches.</div></div></div></div></div> <div>Temps moyen nécessair e pour terminer les opérations d'écriture en une minute. Utilisez cette métrique pour surveiller la I/O latence moyenne des volumes EBS attachés à vos instances Amazon EC2. La moyenne est calculée sur la base I/O des opérations effectuées au cours de la dernière minute. Si aucune opération n'a été effectuée au cours de la</div>	Millisecondes	VolumeId InstanceI d	Minimum Maximum

Métrique	Description	Unités	Dimensions	Statistiques significatives
	<p>dernière minute, la valeur de la métrique est zéro.</p> <p>Pour les volumes Multi-Attach activés, utilisez la InstanceId dimension pour afficher la latence moyenne pour un attachement d'instance de volume spécifique.</p>			

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeIOPSExceededCheck *	<div>  Note Pris en charge pour tous les types de volumes, à l'exception de magnetic (standard), attaché aux instances Nitro. Non pris en charge avec les volumes Multi-Attach activés. Non publié pour les volumes associés à Amazon ECS et AWS Fargate les tâches. </div>	Aucune	VolumeId InstanceId	<ul style="list-style-type: none"> • Sum • Average • Minimum • Maximum
Indique si une application a constamment tenté de générer des IOPS supérieures aux performances IOPS provisionnées du volume au cours de la dernière minute. Cette métrique peut être soit 0 (IOPS provisionnées non				

Métrique	Description	Unités	Dimensions	Statistiques significatives
----------	-------------	--------	------------	-----------------------------

dépassées) soit 1 (IOPS provisionnées dépassées). Pour de plus amples informations, veuillez consulter [Surveillez les I/O caractéristiques à l'aide CloudWatch](#).

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeThroughputExceededCheck *	<div>  Note Pris en charge pour tous les types de volumes, à l'exception de magnetic (standard), attaché aux instances Nitro. Non pris en charge avec les volumes Multi-Attach activés. Non publié pour les volumes associés à Amazon ECS et AWS Fargate les tâches. </div> <p>Indique si une application a constamment tenté de générer un débit supérieur aux performances de débit provisionnées du volume au cours de la dernière minute. Cette métrique peut être soit 0 (débit provisionné non dépassé) soit 1 (débit</p>	Aucune	VolumeId InstanceId	<ul style="list-style-type: none"> • Sum • Average • Minimum Maximum

Métrique	Description	Unités	Dimensions	Statistiques significatives
	provisionné dépassé). Pour plus d'informations, consultez. Surveillez les I/O caractéristiques à l'aide CloudWatch			

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeReadBytes	<p>Fournit des informations sur les opérations de lecture au cours d'une période donnée.</p> <ul style="list-style-type: none"> Les rapports statistiques Sum indiquent le nombre total d'octets transférés pendant la période. La Average statistique indique le nombre moyen d'octets lus au cours de la période spécifiée. La SampleCount statistique représente le nombre de points de données utilisés dans le calcul statistique. 	Octets	VolumeId	<ul style="list-style-type: none"> Average Sum SampleCount Minimum Maximum — uniquement pour les volumes attachés à des Nitro-based instances

 **Note**
 Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité de lecture se

Métrique	Description	Uunités	Dimension s	Statistiq ues significa tives
	produit sur le volume.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeWriteBytes	<p>Fournit des informations sur les opérations d'écriture au cours d'une période donnée.</p> <ul style="list-style-type: none"> Les rapports statistiques Sum indiquent le nombre total d'octets transférés pendant la période. La Average statistique indique le nombre moyen d'octets écrits au cours de la période spécifiée. La SampleCount statistique représente le nombre de points de données utilisés dans le calcul statistique. <div>  Note Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité d'écriture se </div>	Octets	VolumeId	<ul style="list-style-type: none"> Average Sum SampleCount Minimum Maximum — uniquement pour les volumes attachés à des Nitro-based instances

Métrique	Description	Unités	Dimensions	Statistiques significatives
	produit sur le volume.			
VolumeReadOps	Nombre total d'opérations de lecture au cours d'une période donnée. Les opérations de lecture sont comptabilisées une fois terminées. Pour calculer la moyenne d'opérations de lecture d'IOPS (IOPS en lecture) pour la période, divisez le nombre total d'opérations de lecture de la période par le nombre de secondes de la période.	Nombre	VolumeId	<ul style="list-style-type: none"> • Average • Sum • Minimum Maximum — uniquement pour les volumes attachés à des Nitro-based instances

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeWriteOps	Nombre total d'opérations d'écriture au cours d'une période donnée. Les opérations d'écriture sont comptées lorsqu'elles sont terminées. Pour calculer la moyenne d'opérations d'écriture d'IOPS (IOPS en écriture) pour la période, divisez le nombre total d'opérations d'écriture de la période par le nombre de secondes de la période.	Nombre	VolumeId	<ul style="list-style-type: none"> • Average • Sum • Minimum Maximum — uniquement pour les volumes attachés à des Nitro-based instances

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeTotalReadTime	<div>  Note Non pris en charge avec les volumes Multi-Attach activés. Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité de lecture se produit sur le volume. </div> <p>Nombre total de secondes passées par toutes les opérations de lecture terminées, au cours d'une période donnée. Si plusieurs demandes sont soumises en même temps, ce total peut être supérieur à la durée de la période. Par exemple, pour une période de 1 minute (60 secondes) : si 150 opérations ont été réalisées au cours de</p>	Secondes	VolumeId	<ul style="list-style-type: none"> Average—non pertinent pour les volumes attachés aux Nitro-based instances Sum Minimum Maximum—uniquement pour les volumes attachés à des Nitro-based instances

Métrique	Description	Uunités	Dimension s	Statistiq ues significa tives
----------	-------------	---------	----------------	--

cette période et que
chaque opération a pris
une seconde, la valeur
serait 150 secondes.

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeTotalWriteTime	<div>  Note Non pris en charge avec les volumes Multi-Attach activés. Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité d'écriture se produit sur le volume. </div> <p>Nombre total de secondes passées par toutes les opérations d'écriture terminées, au cours d'une période donnée. Si plusieurs demandes sont soumises en même temps, ce total peut être supérieur à la durée de la période. Par exemple, pour une période de 1 minute (60 secondes) : si 150 opérations ont été réalisées au cours de</p>	Secondes	VolumeId	<ul style="list-style-type: none"> Average — non pertinent pour les volumes attachés aux Nitro-based instances Sum Minimum Maximum — uniquement pour les volumes attachés à des Nitro-based instances

Métrique	Description	Uunités	Dimension s	Statistiq ues significa tives
	cette période et que chaque opération a pris une seconde, la valeur serait 150 secondes.			
VolumeIdleTime	<div><div><div><div><div><div></div><div>Note</div></div><div>Non pris en charge avec les volumes Multi-Attach activés.</div></div></div></div><div>Nombre total de secondes dans une période données, alors qu'aucune opération de lecture ou écriture n'a été soumise.</div></div>	Secondes	VolumeId	<div><div>• Average—non pertinent pour les volumes attachés aux Nitro-based instances</div><div>• Sum</div><div>• Minimum Maximum — uniquement pour les volumes attachés à des Nitro-based instances</div></div>

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeQueueLength	Nombre de demandes d'opérations de lecture et d'écriture en attente de réalisation au cours d'une période donnée.	Nombre	VolumeId	<ul style="list-style-type: none"> Average Sum : non pertinent pour les volumes attachés à des instances Nitro Minimum Maximum : uniquement pour les volumes attachés à des instances Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeStatusCheck *	<div>  Note Pour les instances Nitro uniquement. Non publié pour les volumes attachés à Amazon ECS et aux tâches AWS Fargate . </div> <p>Indique si un volume a réussi ou échoué lors d'une vérification d'E/S bloquée au cours de la dernière minute. Cette métrique peut être (réussite) ou 0 1 (échec). Pour de plus amples informations, veuillez consulter Surveillez les I/O caractéristiques à l'aide CloudWatch.</p>	Aucune	VolumeId InstanceId	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeThroughputPercentage	<div>  Note Volumes SSD IOPS provisionnés uniquement. Non pris en charge avec les volumes Multi-Attach activés. </div> <p>Le pourcentage d' I/O opérations par seconde (IOPS) délivrées par rapport au total des IOPS provisionnées pour un volume Amazon EBS. Les volumes SSD IOPS provisionnés fournissent leurs performances provisionnées 99,9 % du temps. Pendant une écriture, s'il n'y a aucune autre I/O demande en attente dans une minute, la valeur de la métrique sera de 100 %. En outre, les I/O performances d'un volume peuvent être temporairement dégradées en raison</p>	Pourcentage	VolumeId	<ul style="list-style-type: none"> Average Minimum Maximum

Métrique	Description	Unités	Dimensions	Statistiques significatives
	d'une action que vous avez entreprise (par exemple, créer un instantané d'un volume pendant les pics d'utilisation, exécuter le volume sur une instance autre que l'EBS-optimized instance ou accéder aux données du volume pour la première fois).			

Métrique	Description	Unités	Dimensions	Statistiques significatives
VolumeConsumedReadWriteOps	<div><div><div>Note</div><div>Volumes SSD IOPS provisionnés uniquement.</div></div></div> <p>Le nombre total d'opérations de lecture et d'écriture (normalisées à 256 000 unités de capacité) consommées au cours d'une période spécifiée. I/O les opérations inférieures à 256 K sont comptées pour 1 IOPS consommée chacune. I/O les opérations supérieures à 256 K sont comptées dans des unités de capacité de 256 000. Par exemple, un 1024 K I/O compterait pour 4 IOPS consommées.</p>	Nombre	VolumeId	<div><div>Average</div><div>Sum</div><div>Minimum</div><div>Maximum</div></div>

Métrique	Description	Unités	Dimensions	Statistiques significatives
BurstBalance	<div>  Note gp2st1, et sc1 volumes uniquement. </div> <p>Fournit des informations sur le pourcentage de I/O crédits (pour gp2) ou de crédits de débit (pour st1 et sc1) restant dans le compartiment de rafale. Les données ne sont communiquées CloudWatch que lorsque le volume est actif. Si le volume n'est pas attaché, aucune donnée n'est présentée. Si les performances de base du volume dépassent les performances en rafale maximales, les crédits ne sont jamais dépensés. Dans d'autres cas, l'équilibre en rafale déclaré est de 100 %. Pour de plus amples informations, veuillez</p>	Pourcentage	VolumeId	<ul style="list-style-type: none"> Average Sum : non pertinent pour les volumes attachés à des instances Nitro. Minimum Maximum

Métrique	Description	Unités	Dimensions	Statistiques significatives
	consulter performance du volume GP2 .			

* Vous ne pouvez pas utiliser ces mesures dans les avant-postes, les zones locales ou les zones de longueur d'onde.

Statistiques pour les instantanés Amazon EBS

L'AWS/EBS espace de noms inclut les mesures suivantes pour les instantanés Amazon EBS.

Métrique	Description	Unités	Dimensions	Statistiques significatives
SnapshotCopyBytesTransferred	La quantité de données de capture d'écran copiées AWS dans une région.	Octets	sourceRegion	Sum

Métriques d'instances Nitro

L'AWS/EC2 espace de noms inclut des métriques Amazon EBS supplémentaires pour les volumes attachés à des Nitro-based instances qui ne sont pas des instances bare metal.

Métrique	Description	Unit	Statistiques significatives
InstanceBSIOPSExc	Indique si une application a tenté de générer des IOPS dépassant les limites maximales d'IOPS EBS pour l'instance au cours de la	Aucune	<ul style="list-style-type: none"> Somme Moyenne Minimum

Métrique	Description	Unit	Statistiques significatives
ReadCheck * *	dernière minute. Cette métrique peut être 0 (IOPS non dépassées) ou 1 (IOPS dépassées).		<ul style="list-style-type: none"> Maximum
InstanceEBSThroughputExceededCheck * *	Indique si une application a tenté de générer un débit dépassant les limites maximales de débit EBS pour l'instance au cours de la dernière minute. Cette métrique peut être 0 (débit non dépassé) ou 1 (débit dépassé).	Aucune	<ul style="list-style-type: none"> Somme Moyenne Minimum Maximum
EBSReadOps	Opérations de lecture terminées de tous les volumes Amazon EBS attachés à l'instance au cours de la période spécifiée. Pour calculer la moyenne I/O des opérations de lecture par seconde (IOPS de lecture) pour la période, divisez le total des opérations de lecture par seconde (IOPS de lecture) pour la période, divisez le total des opérations de lecture par seconde de cette période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour calculer les IOPS en lecture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique <code>DIFF_TIME</code> pour trouver les opérations par seconde. Par exemple, si vous avez représenté graphiquement <code>EBSReadOps</code> en CloudWatch tant que <code>m1</code> , la formule mathématique <code>m1/(DIFF_TIME(m1))</code> renvoie la métrique en opérations/seconde. Pour plus d'informations sur les fonctions mathématiques métriques <code>DIFF_TIME</code> et d'autres fonctions mathématiques, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Nombre	<ul style="list-style-type: none"> Somme Moyenne Minimum Maximum

Métrique	Description	Unit	Statistiques significatives
EBSWriteOps	Opérations d'écriture terminées de tous les volumes EBS attachés à l'instance au cours de la période spécifiée. Pour calculer la moyenne I/O des opérations d'écriture par seconde (IOPS d'écriture) pour la période, divisez le total des opérations de la période par le nombre de secondes de cette période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour calculer les IOPS en écriture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour trouver les opérations par seconde. Par exemple, si vous avez représenté graphiquement EBSWriteOps en CloudWatch tant que <code>m1</code> , la formule mathématique <code>m1/(DIFF_TIME(m1))</code> renvoie la métrique en opérations/seconde. Pour plus d'informations sur les fonctions mathématiques métriques DIFF_TIME et d'autres fonctions mathématiques, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Nombre	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unit	Statistiques significatives
EBSReadBytes	<p>Octets lus de tous les volumes EBS attachés à l'instance au cours de la période spécifiée. Le nombre mentionné correspond au nombre d'octets lus pendant la période. Si vous utilisez la surveillance de base (5 minutes), vous pouvez diviser ce nombre par 300 pour trouver Read Bytes/second. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour trouver les octets par seconde. Par exemple, si vous avez représenté graphiquement EBSReadBytes en CloudWatch tant que m1, la formule mathématique $m1 / (DIFF_TIME(m1))$ renvoie la métrique en bytes/second. Pour plus d'informations sur les fonctions mathématiques métriques DIFF_TIME et d'autres fonctions mathématiques, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Octets	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unit	Statistiques significatives
EBSWriteBytes	<p>Octets écrits dans tous les volumes EBS attachés à l'instance au cours de la période spécifiée. Le nombre mentionné correspond au nombre d'octets écrits pendant la période. Si vous utilisez la surveillance de base (5 minutes), vous pouvez diviser ce nombre par 300 pour trouver Write Bytes/second. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique DIFF_TIME pour trouver les octets par seconde. Par exemple, si vous avez représenté graphiquement EBSWriteBytes en CloudWatch tant que m1, la formule mathématique métrique $m1 / (\text{DIFF_TIME}(m1))$ renvoie la métrique en bytes/second. Pour plus d'informations sur les fonctions mathématiques métriques DIFF_TIME et d'autres fonctions mathématiques, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.</p>	Octets	<ul style="list-style-type: none"> • Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unit	Statistiques significatives
EBSIOBalance%	<p>Fournit des informations sur le pourcentage de I/O crédits restant dans le compartiment Burst. Cette métrique est disponible uniquement pour la surveillance basique. Cette métrique n'est disponible que pour certaines tailles d'instance *.4xlarge et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures. Pour plus d'informations, consultez la section EBS optimisé par défaut.</p> <p>La statistique Sum n'est pas applicable pour cette métrique.</p>	Pourcentage	<ul style="list-style-type: none"> • Minimum • Maximum
EBSByteBalance%	<p>Fournit des informations sur le pourcentage de crédits de débit restant dans le compartiment en rafales. Cette métrique est disponible uniquement pour la surveillance basique. Cette métrique n'est disponible que pour certaines tailles d'instance *.4xlarge et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures. Pour plus d'informations, consultez la section EBS optimisé par défaut.</p> <p>La statistique Sum n'est pas applicable pour cette métrique.</p>	Pourcentage	<ul style="list-style-type: none"> • Minimum • Maximum

* Vous ne pouvez pas utiliser ces mesures dans les avant-postes, les zones locales ou les zones de longueur d'onde.

Métriques de restauration d'instantané rapide

L'espace de noms AWS/EBS inclut les métriques suivantes pour une [restauration d'instantané rapide](#).

Métrique	Description	Unités	Dimensions	Statistiques significatives
FastSnapshotRestoreCreditsBucketSize	Nombre maximum de crédits de création de volume pouvant être accumulés. Cette métrique est signalée par instantané et par zone de disponibilité.	Aucune	SnapshotId AvailabilityZone	<ul style="list-style-type: none"> Average Minimum Maximum <div>  Note La statistique la plus significative est Average. Les résultats des statistiques Minimum et Maximum sont les mêmes que ceux de Average et peuvent être utilisés indifféremment. </div>
FastSnapshotRestoreCreditsBalance	Nombre de crédits de création de volume disponibles. Cette métrique est signalée par instantané et par zone de disponibilité.	Aucune	SnapshotId AvailabilityZone	<ul style="list-style-type: none"> Average Minimum Maximum <div>  Note La statistique la plus significative est Average. Les résultats des statistiques Minimum et Maximum sont les mêmes que ceux de Average </div>

Métrique	Description	Unités	Dimensions	Statistiques significatives
				et peuvent être utilisés indifféremment.

Graphiques de la console Amazon EC2

Après avoir créé un volume, vous pouvez afficher les graphiques de surveillance du volume dans la console Amazon EC2. Sélectionnez un volume dans la page Volumes de la console, puis sélectionnez Surveillance. Le tableau ci-après répertorie les graphiques affichés. La colonne de droite décrit la manière dont les métriques de données brutes de l' CloudWatch API sont utilisées pour produire chaque graphique. La période de tous les graphiques est de 5 minutes.

Graphique	Description de l'utilisation des métriques brutes
Débit de lecture (KiB/s)	$\text{Sum}(\text{VolumeReadBytes}) / \text{Period} / 1024$
Débit d'écriture (KiB/s)	$\text{Sum}(\text{VolumeWriteBytes}) / \text{Period} / 1024$
Opérations de lecture (Ops/s)	$\text{Sum}(\text{VolumeReadOps}) / \text{Period}$
Opérations d'écriture (Ops/s)	$\text{Sum}(\text{VolumeWriteOps}) / \text{Period}$
Longueur moyenne de la file d'attente (Opérations)	$\text{Avg}(\text{VolumeQueueLength})$
Temps inactif (%)	$\text{Sum}(\text{VolumeIdleTime}) / \text{Period} \times 100$
Taille de lecture moyenne (KiB/op)	$\text{Avg}(\text{VolumeReadBytes}) / 1024$ Par exemple Nitro-based , la formule suivante calcule la taille de lecture moyenne à l'aide des mathématiques CloudWatch métriques : $(\text{Sum}(\text{VolumeReadBytes}) / \text{Sum}(\text{VolumeReadOps})) / 1024$

Graphique	Description de l'utilisation des métriques brutes
	<p>Les VolumeReadOps métriques VolumeReadBytes et sont disponibles dans la CloudWatch console EBS.</p>
<p>Taille d'écriture moyenne (KiB/op)</p>	<p>$\text{Avg}(\text{VolumeWriteBytes}) / 1024$</p> <p>Par exemple Nitro-based , la formule suivante calcule la taille d'écriture moyenne à l'aide des mathématiques CloudWatch métriques :</p> <p>$(\text{Sum}(\text{VolumeWriteBytes}) / \text{Sum}(\text{VolumeWriteOps})) / 1024$</p> <p>Les VolumeWriteOps métriques VolumeWriteBytes et sont disponibles dans la CloudWatch console EBS.</p>
<p>Latence de lecture moyenne (ms/op)</p>	<p>$\text{Avg}(\text{VolumeTotalReadTime}) \times 1000$</p> <p>Par exemple Nitro-based , la formule suivante calcule la latence de lecture moyenne à l'aide de CloudWatch Metric Math :</p> <p>$(\text{Sum}(\text{VolumeTotalReadTime}) / \text{Sum}(\text{VolumeReadOps})) \times 1000$</p> <p>Les VolumeReadOps métriques VolumeTotalReadTime et sont disponibles dans la CloudWatch console EBS.</p>

Graphique	Description de l'utilisation des métriques brutes
Latence d'écriture moyenne (ms/op)	$\text{Avg}(\text{VolumeTotalWriteTime}) \times 1000$ <p>Par exemple Nitro-based , la formule suivante calcule la latence d'écriture moyenne à l'aide des mathématiques CloudWatch métriques :</p> $(\text{Sum}(\text{VolumeTotalWriteTime}) / \text{Sum}(\text{VolumeWriteOps})) * 1000$ <p>Les VolumeWriteOps métriques VolumeTotalWriteTime et sont disponibles dans la CloudWatch console EBS.</p>

Pour les graphiques de latence moyenne et ceux de taille moyenne, la moyenne est calculée par rapport au nombre total d'opérations (lecture ou écriture, quel que soit celui applicable au graphe) complétées durant la période.

EventBridge Événements Amazon pour Amazon EBS

Amazon EBS envoie des événements à Amazon EventBridge pour les actions effectuées sur les volumes et les instantanés. Avec EventBridge, vous pouvez établir des règles qui déclenchent des actions programmatiques en réponse à ces événements. Par exemple, vous pouvez créer une règle qui envoie une notification sur votre adresse électronique lorsqu'un instantané est activé pour une restauration rapide des instantanés.

Les événements dans EventBridge sont représentés sous forme d'objets JSON. Les champs spécifiques à l'événement figurent dans la section « détail » de l'objet JSON. Le champ « événement » contient le nom de l'événement. Le champ « résultat » contient l'état terminé de l'action qui déclenche l'événement. Pour plus d'informations, consultez les modèles EventBridge d'événements [Amazon](#) dans le guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations, consultez [Qu'est-ce qu'Amazon EventBridge ?](#) dans le guide de EventBridge l'utilisateur Amazon.

Événements

- [Événements de volume EBS](#)

- [Événement d'initialisation du volume EBS](#)
- [Événements de modification de volume EBS](#)
- [Événements d'instantané EBS](#)
- [Événements d'archivage d'instantanés EBS](#)
- [Événements de restauration d'instantané rapide EBS](#)
- [Utilisation AWS Lambda pour gérer les EventBridge événements](#)

Événements de volume EBS

Amazon EBS envoie des événements EventBridge lorsque les événements de volume suivants se produisent.

Événements

- [Créer un volume \(createVolume\)](#)
- [Supprimer le volume \(deleteVolume\)](#)
- [Attacher ou réattacher le volume \(attachVolume, reattachVolume\)](#)
- [Détacher le volume \(DetachVolume\)](#)

Créer un volume (createVolume)

L'`createVolume` événement est envoyé à votre AWS compte lorsqu'une action visant à créer un volume est terminée. Cependant, il n'est pas enregistré, enregistré ou archivé. Cet événement peut avoir le résultat `available` ou `failed`. La création échouera si une valeur non valide AWS KMS key a été fournie, comme indiqué dans les exemples ci-dessous.

Données d'événement

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS pour un événement `createVolume` réussi.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
```



```

"region": "us-east-1",
"resources": [
  "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
],
"detail": {
  "result": "available",
  "cause": "",
  "event": "createVolume",
  "request-id": "01234567-0123-0123-0123-0123456789ab"
}
}

```

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS après un événement `createVolume` ayant échoué. La cause de l'échec est attribuée à une clé KMS désactivée.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}

```

Voici un exemple d'objet JSON émis par EBS après un événement `createVolume` ayant échoué. La cause de l'échec est attribuée à l'importation en attente d'une clé KMS.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",

```

```

"source": "aws.ec2",
"account": "012345678901",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "sa-east-1",
"resources": [
  "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
],
"detail": {
  "event": "createVolume",
  "result": "failed",
  "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
  "request-id": "01234567-0123-0123-0123-0123456789ab",
}
}

```

Supprimer le volume (deleteVolume)

L'event deleteVolume est envoyé à votre AWS compte lorsqu'une action visant à supprimer un volume est terminée. Cependant, il n'est pas enregistré, enregistré ou archivé. Le résultat de cet événement est deleted. Si la suppression ne se termine pas, l'événement n'est pas envoyé.

Données d'événement

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS pour un événement deleteVolume réussi.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
  ],
  "detail": {
    "result": "deleted",
    "cause": "",
    "event": "deleteVolume",
    "request-id": "01234567-0123-0123-0123-0123456789ab"
  }
}

```

```
}
}
```

Attacher ou réattacher le volume (attachVolume, reattachVolume)

L'événement `attachVolume` est envoyé à votre AWS compte lorsqu'un volume est attaché ou rattaché à une instance. Cependant, il n'est pas enregistré, enregistré ou archivé. Si vous utilisez une clé KMS pour chiffrer un volume EBS et que la clé KMS devient non valide, EBS émet un événement si cette clé KMS est utilisée ultérieurement pour l'attachement ou le rattachement d'une instance, comme illustré dans les exemples ci-dessous.

Données d'événement

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS après un événement `attachVolume` ayant échoué. La cause de l'échec est attribuée à la suppression en attente d'une clé KMS.

Note

AWS peut tenter de se reconnecter à un volume après une maintenance de routine du serveur.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
    "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

```
}
}
```

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS après un événement `reattachVolume` ayant échoué. La cause de l'échec est attribuée à la suppression en attente d'une clé KMS.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
    "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

Détacher le volume (DetachVolume)

L'`detachVolume` événement est envoyé à votre AWS compte lorsqu'un volume est détaché d'une instance Amazon EC2.

Données d'événement

Voici un exemple d'`detachVolume` événement réussi.

```
{
  "version": "0",
  "id": "2ec37298-1234-e436-70fc-c96b1example",
  "detail-type": "AWS API Call via CloudTrail",
  "source": "aws.ec2",
  "account": "123456789012",
```

```

"time":"2024-03-18T16:35:52Z",
"region":"us-east-1",
"resources":[],
"detail":
{
  "eventVersion":"1.09",
  "userIdentity":
  {
    "type":"IAMUser",
    "principalId":"AIDAJT12345SQ2EXAMPLE",
    "arn":"arn:aws:iam::123456789012:user/administrator",
    "accountId":"123456789012",
    "accessKeyId":"AKIAJ67890A6EXAMPLE",
    "userName":"administrator"
  },
  "eventTime":"2024-03-18T16:35:52Z",
  "eventSource":"ec2.amazonaws.com",
  "eventName":"DetachVolume",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"12.12.123.12",
  "userAgent":"aws-cli/2.7.12 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/ec2.detach-volume",
  "requestParameters":
  {
    "volumeId":"vol-072577c46bexample",
    "force":false
  },
  "responseElements":
  {
    "requestId":"1234513a-6292-49ea-83f8-85e95example",
    "volumeId":"vol-072577c46bexample",
    "instanceId":"i-0217f7eb3dexample",
    "device":"/dev/sdb",
    "status":"detaching",
    "attachTime":1710776815000
  },
  "requestID":"1234513a-6292-49ea-83f8-85e95example",
  "eventID":"1234551d-a15a-43eb-9e69-c983aexample",
  "readOnly":false,
  "eventType":"AwsApiCall",
  "managementEvent":true,
  "recipientAccountId":"123456789012",
  "eventCategory":"Management",
  "tlsDetails":

```

```
{
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
}
```

Événement d'initialisation du volume EBS

Lorsque vous créez un volume Amazon EBS à partir d'un instantané et que vous utilisez le taux d'initialisation du volume par défaut ou un taux provisionné Amazon EBS pour l'initialisation du volume, l'`initializeVolume` événement est envoyé à votre AWS compte dans les cinq minutes suivant la fin de l'initialisation du volume. Pour de plus amples informations, veuillez consulter [Utiliser un tarif provisionné par Amazon EBS pour l'initialisation des volumes](#).

L'événement n'est pas envoyé pour les volumes créés à l'aide de Fast Snapshot Restore.

Important

`completionTime` reflète la date à laquelle l'événement a été généré. Étant donné que l'événement est généré dans les 5 minutes suivant la fin de l'initialisation, il `completionTime` peut s'écouler jusqu'à cinq minutes après la fin de l'initialisation.

Voici un exemple d'événement.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567890abcdef"
  ],
  "detail": {
    "event": "initializeVolume",
    "result": "succeeded",
```

```

    "completionTime": "yyyy-mm-ddThh:mm:ssZ",
    "request-id": "01234567-0123-0123-0123-0123456789ab"
  }
}

```

Événements de modification de volume EBS

Amazon EBS envoie modifyVolume des événements EventBridge lorsqu'un volume est modifié. Cependant, il n'est pas enregistré, enregistré ou archivé.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
  ],
  "detail": {
    "result": "optimizing",
    "cause": "",
    "event": "modifyVolume",
    "request-id": "01234567-0123-0123-0123-0123456789ab"
  }
}

```

Événements d'instantané EBS

Amazon EBS envoie des événements EventBridge lorsque les événements de volume suivants se produisent.

Événements

- [Créer un instantané \(createSnapshot\)](#)
- [Créer des instantanés \(createSnapshots\)](#)
- [Copier un instantané \(copySnapshot\)](#)
- [Partager un instantané \(shareSnapshot\)](#)

Créer un instantané (createSnapshot)

L'createSnapshot événement est envoyé à votre AWS compte lorsqu'une action visant à créer un instantané est terminée. Cependant, il n'est pas enregistré, enregistré ou archivé. Cet événement peut avoir le résultat succeeded ou failed.

Données d'événement

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS pour un événement createSnapshot réussi. Dans la section detail, le champ source contient l'ARN du volume source. Les champs startTime et endTime indiquent le moment où la création de l'instantané a commencé et est terminée.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"  }
}
```

Créer des instantanés (createSnapshots)

L'createSnapshots événement est envoyé à votre AWS compte lorsqu'une action visant à créer un instantané en plusieurs volumes est terminée. Cet événement peut avoir le résultat succeeded ou failed.

Données d'événement

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS pour un événement `createSnapshots` réussi. Dans la section `detail`, le champ `source` contient les ARN des volumes sources de l'ensemble d'instantanés multi-volumes. Les champs `startTime` et `endTime` indiquent le moment où la création de l'instantané a commencé et est terminée.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-01234568"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "completed"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234568",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234568",
        "status": "completed"
      }
    ]
  }
}
```

La liste ci-dessous est l'exemple d'un objet JSON émis par EBS après un événement `createSnapshots` ayant échoué. La cause de l'échec correspondait à un ou plusieurs instantanés de l'ensemble d'instantanés multi-volumes qui n'ont pas pu aboutir. Les valeurs de `snapshot_id`

sont les ARN des instantanés qui ont échoué. `startTime` et `endTime` représentent les instants où l'action de création de l'instantané a commencé et s'est terminée.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-01234568"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "error"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234568",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234568",
        "status": "error"
      }
    ]
  }
}
```

Copier un instantané (copySnapshot)

L'`copySnapshot` événement est envoyé à votre AWS compte lorsqu'une action visant à copier un instantané est terminée. Cependant, il n'est pas enregistré, enregistré ou archivé. Cet événement peut avoir le résultat `succeeded` ou `failed`.

Dans la `detail` section, `source` se trouvent l'ARN de l'instantané source et `snapshot_id` l'ARN de la copie du cliché. `startTime` et `endTime` indiquent quand l'opération de copie a commencé et s'est terminée. `incremental` indique si la copie de l'instantané est un instantané incrémentiel (`true`) ou un instantané complet (`false`). `transferType` indique si l'opération de copie instantanée était une opération de copie standard ou une opération de copie basée sur le temps. Pour de plus amples informations, veuillez consulter [Time-based copies pour les instantanés et les AMI Amazon EBS EBS-backed](#).

Si vous copiez l'instantané d'une région à l'autre, l'événement est émis dans la région de destination.

Scénario 1 : l'opération de copie d'un instantané standard est terminée

Voici un exemple d'événement envoyé à votre compte lorsqu'une opération de copie d'instantané standard s'est terminée avec succès. Notez que `transferType` est `standard`.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "incremental": "true",
    "transferType": "standard"
  }
}
```

Scénario 2 : l'opération de copie du Time-based snapshot se termine dans les délais impartis

Voici un exemple d'événement envoyé à votre compte lorsqu'une opération de copie d'instantanés basée sur le temps est terminée dans les délais impartis. Notez que `transferType` indique qu'il s'agissait d'une opération de copie d'instantané basée sur le temps. `time-based completionDurationStartTime` indique à quel moment la durée de réalisation a commencé.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime": "2024-11-16T06:27:33.816Z",
    "transferType": "time-based"
  }
}
```

Scénario 3 : l'opération de copie des Time-based instantanés se termine mais ne respecte pas le délai d'exécution demandé

Lorsqu'une opération de copie d'instantanés basée sur le temps est terminée, mais qu'elle ne respecte pas la durée requise, CloudWatch deux événements sont envoyés à votre compte. Voici des exemples de ces événements.

- Le premier événement est envoyé à votre compte dès que la durée de réalisation est dépassée, même si l'opération de copie est toujours en cours. Pour cet événement, le `detail-type` est EBS

Copy Snapshot Missed Completion Duration et `missedCompletionDurationCause` fournit la raison.

```
{
  "version": "0",
  "id": "fd90eb95-0938-e02c-cf55-b81363b8ac12",
  "detail-type": "EBS Copy Snapshot Missed Completion Duration",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2024-11-19T18:17:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:123456789012:snapshot/snap-01234567890abcdef"],
  "detail": {
    "event": "copySnapshot",
    "missedCompletionDurationCause": "Snapshot copy was not able to meet the specified completion duration because your snapshot copy operation throughput quota was exceeded.",
    "snapshot_id": "arn:aws:ec2:us-east-1:123456789012:snapshot/snap-01234567890abcdef",
    "source": "arn:aws:ec2:us-east-1:123456789012:snapshot/snap-00987654321fedcba",
    "startTime": "Sun Nov 24 22:32:55 UTC 2024",
    "transferType": "time-based"
  }
}
```

- Le deuxième événement n'est envoyé à votre compte qu'une fois la capture d'écran terminée. L'événement inclut `missedCompletionDurationCause`, ce qui en fournit la raison.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
  }
}
```

```

    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime": "2024-11-16T06:27:33.816Z",
    "missedCompletionDurationCause": "Snapshot copy was not able to meet the specified completion duration because your snapshot copy operation throughput quota was exceeded.",
    "transferType": "time-based"
  }
}

```

Scénario 4 : échec de l'opération de copie du snapshot

Voici un exemple d'événement envoyé à votre compte en cas d'échec d'une opération de copie d'instantané. Notez que `result` c'est `failed` pour indiquer que l'opération a échoué.

```

{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}

```

Partager un instantané (shareSnapshot)

L'event shareSnapshot est envoyé à votre AWS compte lorsqu'un autre compte partage une capture d'écran avec celui-ci. Cependant, il n'est pas enregistré, enregistré ou archivé. Le résultat est toujours succeeded.

Données d'événement

Ce qui suit est un exemple d'objet JSON émis par EBS après un événement shareSnapshot terminé. Dans cette section, la valeur de source est le numéro de compte AWS de l'utilisateur qui a partagé l'instantané avec vous. startTime et endTime représentent le début et la fin de l'action share-snapshot. L'événement shareSnapshot est émis uniquement lorsqu'un instantané privé est partagé avec un autre utilisateur. Le partage d'un instantané public ne déclenche pas l'événement.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "012345678901",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Événements d'archivage d'instantanés EBS

Amazon EBS émet des événements liés aux actions d'archivage des instantanés. Pour plus d'informations, voir [Surveillez l'archivage des instantanés Amazon EBS à l'aide d'événements CloudWatch](#).

Événements de restauration d'instantané rapide EBS

Amazon EBS envoie des événements EventBridge lorsque l'état de restauration rapide d'un instantané change. Les événements sont générés dans la mesure du possible.

Voici un exemple de données pour cet événement.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Fast Snapshot Restore State-change Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
  ],
  "detail": {
    "snapshot-id": "snap-1234567890abcdef0",
    "state": "optimizing",
    "zone": "us-east-1a",
    "message": "Client.UserInitiated - Lifecycle state transition",
  }
}
```

Les valeurs possibles pour state sont enabling, optimizing, enabled, disabling et disabled.

Les valeurs possibles pour message sont les suivantes :

`Client.InvalidSnapshot.InvalidState` - The requested snapshot transitioned to an invalid state (Error)

Une demande d'activation de la fonction de restauration d'instantané rapide a échoué et l'état est passé à `disabling` ou `disabled`. La fonction de restauration d'instantané rapide ne peut pas être activée pour cet instantané.

`Client.UserInitiated`

L'état est passé avec succès à `enabling` ou `disabling`.

`Client.UserInitiated` - Lifecycle state transition

L'état est passé avec succès à `optimizing`, `enabled` ou `disabled`.

`Server.InsufficientCapacity` - There was insufficient capacity available to satisfy the request

Une demande d'activation de la fonction de restauration d'instantané rapide a échoué en raison d'une capacité insuffisante et l'état est passé à `disabling` ou `disabled`. Attendez, puis recommencez.

`Server.InternalError` - An internal error caused the operation to fail

Une demande d'activation de la fonction de restauration d'instantané rapide a échoué en raison d'une erreur interne et l'état est passé à `disabling` ou `disabled`. Attendez, puis recommencez.

`Client.InvalidSnapshot.InvalidState` - The requested snapshot was deleted or access permissions were revoked

L'état de restauration d'instantané rapide est passé à `disabling` ou `disabled` parce que l'instantané a été supprimé ou non partagé par son propriétaire. La restauration d'instantané rapide ne peut pas être activée pour un instantané qui a été supprimé ou qui n'est plus partagé avec vous.

Utilisation AWS Lambda pour gérer les EventBridge événements

Vous pouvez utiliser Amazon EBS et Amazon EventBridge pour automatiser votre flux de sauvegarde des données. Pour cela, vous devez créer une politique IAM, une AWS Lambda fonction pour gérer l'événement et une EventBridge règle qui fait correspondre les événements entrants et les achemine vers la fonction Lambda.

La procédure suivante utilise l'événement `createSnapshot` pour copier automatiquement un instantané terminé vers une autre région pour la reprise après sinistre.

Pour copier un instantané terminé vers une autre région

1. Créez une politique IAM, telle que celle illustrée dans l'exemple suivant, pour fournir les autorisations nécessaires pour utiliser l'`CopySnapshot` action et écrire dans le EventBridge journal. Attribuez la politique à l'utilisateur qui gèrera l' EventBridge événement.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Définissez une fonction dans Lambda qui sera disponible depuis la EventBridge console. L'exemple de fonction Lambda ci-dessous, écrit en Node.js, est invoqué EventBridge lorsqu'un `createSnapshot` événement correspondant est émis par Amazon EBS (ce qui signifie qu'un instantané a été réalisé). Lorsqu'elle est appelée, la fonction copie l'instantané de `us-east-2` vers `us-east-1`.

```
// Sample Lambda function to copy an EBS snapshot to a different Region
```

```
var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
    initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
        } else {
            const successMessage = `Successfully started copy of snapshot
${snapshotId} to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
}
```

```
    }  
  });  
};
```

Pour vous assurer que votre fonction Lambda est disponible depuis la EventBridge console, créez-la dans la région où l' EventBridge événement se produira. Pour plus d'informations, consultez le [Guide du développeur AWS Lambda](#).

3. Ouvrez la EventBridge console Amazon à l'adresse <https://console.aws.amazon.com/events/>.
4. Dans le volet de navigation, sélectionnez Rules (Règles), puis Create rule (Créer une règle).
5. Pour Step 1: Define rule detail (Étape 1 : Définir les détails de la règle), procédez comme suit :
 - a. Saisissez un Name (Nom) et une Description pour la règle.
 - b. Pour Event bus (Bus d'événements), gardez default (par défaut).
 - c. Assurez-vous que l'option Activer la règle sur le bus d'événements sélectionné est activée.
 - d. Pour Event type (Type d'événement), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
 - e. Choisissez Suivant.
6. Pour Step 2: Build event pattern (Étape 2 : Créer un modèle d'événement), procédez comme suit :
 - a. Dans Source de l'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
 - b. Dans la section Modèle d'événement, pour Source de l'événement, assurez-vous que le AWS service est sélectionné, et pour le AWS service, sélectionnez EC2.
 - c. Pour Event type (Type d'événement), sélectionnez EBS Snapshot Notification (Notification Instantanée EBS), Specific event(s) (Événement(s) spécifique), puis choisissez createSnapshot.
 - d. Sélectionnez Specific result(s) (Résultat(s) spécifique(s)), puis choisissez succeeded.
 - e. Choisissez Suivant.
7. Pour Step 3: Select targets (Étape 3 : Sélectionner les cibles), procédez comme suit :
 - a. Pour Types de cibles, choisissez service AWS .
 - b. Pour Select target (Sélectionner la cible), choisissez Lambda function (Fonction Lambda), et pour Fonction, sélectionnez la fonction que vous avez créée précédemment.
 - c. Choisissez Next (Suivant)

8. Pour Step 4: Configure tags (Étape 4 : Configurer les balises), spécifiez des balises pour la règle si nécessaire, puis choisissez Next (Suivant).
9. Pour Step 5: Review and create (Étape 5 : Examen et création), passez en revue la règle, puis choisissez Create rule (Créer une règle).

Votre règle doit désormais apparaître sur l'onglet Rules. Dans l'exemple présenté, l'événement que vous avez configuré doit être émis par EBS la prochaine fois que vous copiez un instantané.

Statistiques de performances détaillées d'Amazon EBS

Les appareils en mode bloc Amazon EBS NVMe fournissent des statistiques de I/O performances haute résolution en temps réel pour les volumes Amazon EBS attachés aux Nitro-based instances Amazon EC2. Ces statistiques sont présentées sous forme de compteurs agrégés qui sont conservés pendant la durée de l'attachement du volume à l'instance. Les statistiques fournissent des détails sur le nombre cumulé d'opérations, les octets envoyés et reçus et le temps consacré aux I/O opérations de lecture et d'écriture. De plus, les statistiques incluent des histogrammes pour les I/O opérations de lecture et d'écriture. Ils indiquent également la durée totale pendant laquelle votre application a dépassé les limites d'IOPS ou de débit provisionnées du volume EBS ou de l'instance attachée.

Vous pouvez collecter ces statistiques avec une granularité allant jusqu'à une seconde d'intervalle. Si les demandes sont effectuées plus fréquemment que des intervalles d'une seconde, le pilote NVMe peut les mettre en file d'attente, ainsi que d'autres commandes d'administration, pour être traitées ultérieurement.

Considérations

- Les statistiques sont prises en charge pour tous les types de volumes Amazon EBS.
- Les statistiques ne sont prises en charge que pour les volumes associés à [des instances créées sur le système AWS Nitro](#).
- Les statistiques sont disponibles pour les volumes Multi-Attach activés. Lorsque vous consultez les statistiques d'un volume Multi-Attach activé, les statistiques sont spécifiques à cette instance jointe et reflètent uniquement l'utilisation de cette instance.
- Les statistiques sont disponibles sans frais supplémentaires.

Statistiques

Le périphérique de blocage Amazon EBS NVMe fournit les statistiques suivantes :

Nom de la statistique	Nom complet	Type	Description
total_read_ops	Nombre total d'opérations	Compteur	Nombre total d'opérations de lecture terminées.
total_write_ops	Nombre total d'opérations d'écriture	Compteur	Nombre total d'opérations d'écriture terminées.
total_read_bytes	Nombre total d'octets lus	Compteur	Nombre total d'octets lus transférés.
total_write_bytes	Nombre total d'octets écrits	Compteur	Nombre total d'octets écrits transférés.
total_read_time	Durée totale de lecture	Compteur	Temps total, en microsecondes, passé pour toutes les opérations de lecture terminées.
total_write_time	Durée totale d'écriture	Compteur	Temps total, en microsecondes, passé pour toutes les opérations d'écriture terminées.
ebs_volume_performance_exceeded_iops	Durée totale pendant laquelle la demande a dépassé le volume provisionné (IOPS)	Compteur	Temps total, en microsecondes, pendant lequel la demande d'IOPS a dépassé les performances d'IOPS provisionnées pour le volume.
ebs_volume_performance_exceeded_tp	Temps total pendant lequel la demande a dépassé le volume et le débit provisionné	Compteur	Temps total, en microsecondes, pendant lequel la demande de débit a dépassé les performances de débit provisionnées pour le volume.
ec2_instance_ebs_performance	Durée totale pendant laquelle la demande a dépassé les	Compteur	Temps total, en microsecondes, pendant lequel le volume EBS a dépassé les performances d'IOPS maximales de l'instance Amazon EC2.

Nom de la statistique	Nom complet	Type	Description
<code>e_exceeded_iops</code>	performances IOPS de l'instance EC2		
<code>ec2_instance_ebs_performance_exceeded_time</code>	Durée totale pendant laquelle la demande a dépassé les performances de débit de l'instance EC2	Compteur	Temps total, en microsecondes, pendant lequel le volume EBS a dépassé le débit maximal de l'instance Amazon EC2.
<code>volume_queue_length</code>	Longueur de la file d'attente de volume	Ponctuelle	Nombre d'opérations de lecture et d'écriture en attente d'exécution.
<code>read_io_latency_histogram</code>	Lire l' I/O histogramme	Histogramme *	Nombre d'opérations de lecture effectuées dans chaque intervalle de latence, en microsecondes.
<code>write_io_latency_histogram</code>	Écrire un I/O histogramme	Histogramme *	Nombre d'opérations d'écriture effectuées dans chaque intervalle de latence, en microsecondes.

Note

* Les statistiques de l'histogramme ne représentent que I/O les opérations qui se sont terminées avec succès. Les I/O opérations bloquées ou altérées ne sont pas incluses, mais elles apparaîtront clairement dans les `volume_queue_length` statistiques, qui sont présentées sous forme de statistiques ponctuelles.

Accès aux statistiques

Les statistiques doivent être accessibles directement depuis l'instance à laquelle le volume Amazon EBS est attaché. Vous pouvez accéder aux statistiques en utilisant l'une des méthodes suivantes.

Instances Linux

Amazon CloudWatch

Vous pouvez configurer l' CloudWatch agent Amazon pour collecter les statistiques de votre instance et les rendre disponibles sous forme de statistiques personnalisées dans CloudWatch. Vous pouvez ensuite utiliser les mesures CloudWatch pour analyser les I/O modèles, suivre les tendances en matière de performances, créer des tableaux de bord personnalisés et configurer des alarmes automatisées en fonction de seuils de performance.

Pour plus d'informations sur la configuration de l' CloudWatch agent, consultez les rubriques suivantes :

- [Création du fichier de configuration de CloudWatch l'agent](#)
- [Collectez les statistiques des pilotes Amazon EBS NVMe](#)

Avec la version complémentaire Amazon CloudWatch Observability EKS 4.1.0 et les versions ultérieures, les statistiques sont automatiquement collectées lorsque les métriques du pilote Amazon EBS CSI sont activées. Pour plus d'informations, consultez les statistiques des pilotes [Amazon EBS NVMe](#).

ebsnvme script

Le ebsnvme script se trouve dans le dépôt Github [amazon-ec2-utils](#).

Pour accéder aux statistiques

1. Connectez-vous à l'instance à laquelle le volume est attaché.
2. Téléchargez le ebsnvme script depuis le amazon-ec2-utils dépôt Github.

```
wget https://raw.githubusercontent.com/amazonlinux/amazon-ec2-utils/refs/heads/main/ebsnvme
```

3. Modifiez les autorisations du script pour le rendre exécutable.


```
sudo chmod +x ./ebsnvme
```

4. Exécutez le ebsnvme script et spécifiez le nom du périphérique pour le volume.

```
sudo ./ebsnvme stats /dev/nvme0n1
```

nvme-cli tool

Pour accéder aux statistiques

1. Connectez-vous à l'instance à laquelle le volume est attaché.
2. Les AMI Amazon Linux publiées après le 12 novembre 2024 incluent la dernière version de l'nvme-clioutil. Si vous utilisez une ancienne AMI Amazon Linux, mettez à jour l'outil nvme-cli.

```
sudo yum install nvme-cli
```

3. Exécutez la commande suivante et spécifiez le nom du périphérique pour le volume.

```
nvme amzn stats /dev/nvme0n1
```

Prometheus

Vous pouvez surveiller les statistiques avec Prometheus, une application de surveillance open source, et Amazon Managed Service pour Prometheus. Cela permet de surveiller plus facilement les volumes Amazon EBS dans les environnements de conteneurs et Kubernetes à grande échelle. Avec la version v1.37.0 et les versions ultérieures du pilote Amazon EBS CSI, les statistiques de performances détaillées sont exposées en tant que Prometheus-compatible / metrics point final pour l'exportation vers Prometheus.

Pour plus d'informations, consultez la section [Ingestion des métriques dans votre espace de travail Amazon Managed Service for Prometheus](#) dans le guide de l'utilisateur d'Amazon Managed Service for Prometheus.

instances Windows

nvme_amzn.exe tool

Pour accéder aux statistiques

1. Connectez-vous à l'instance à laquelle le volume est attaché.
2. Assurez-vous que vous utilisez la version du pilote AWSNVMe version 1.7.0 ou ultérieure. Pour plus d'informations sur la mise à jour du pilote AWSNVMe, consultez la section [Pilotes NVMe AWS](#).
3. Obtenez le numéro de disque du volume EBS. Pour plus d'informations, voir Associer [les volumes Amazon EBS aux noms de périphériques NVMe](#)
4. Exécutez la commande suivante en tant qu'administrateur et spécifiez le numéro de disque du volume.

```
.\nvme_amzn.exe stats disk_number
```

Amazon GuardDuty pour Amazon EBS

Amazon GuardDuty est un service de détection des menaces qui aide à protéger vos comptes, vos conteneurs, vos charges de travail et les données de votre AWS environnement. À l'aide de modèles d'apprentissage automatique (ML) et de capacités de détection des anomalies et des menaces, vous surveillez GuardDuty en permanence les différentes sources de journaux et l'activité d'exécution afin d'identifier et de hiérarchiser les risques de sécurité potentiels et les activités malveillantes dans votre environnement.

La fonctionnalité [Malware Protection](#) intégrée GuardDuty analyse les volumes Amazon EBS associés à vos instances Amazon EC2 et à vos charges de travail de conteneur afin de détecter les menaces potentielles. GuardDuty propose deux méthodes pour ce faire :

- Activer la protection contre les programmes malveillants : lorsqu'il GuardDuty génère un résultat indiquant la présence potentielle d'un logiciel malveillant dans une instance Amazon EC2 ou une charge de travail de conteneur, il lance automatiquement une analyse des programmes malveillants sur la ressource potentiellement compromise.
- Utilisez l'analyse des programmes malveillants à la demande sans activer la protection contre les programmes malveillants : fournissez le nom de ressource Amazon (ARN) de votre instance Amazon EC2 pour lancer une analyse à la demande.

Pour plus d'informations, consultez le [guide de GuardDuty l'utilisateur Amazon](#).

Comprendre les codes d'Amazon EBS dans les rapports de facturation et d'utilisation

Lorsque vous utilisez Amazon EBS, nous incluons les codes associés dans vos rapports AWS de facturation et d'utilisation. L'examen de ces codes vous aide à comprendre les coûts et les habitudes d'utilisation d'Amazon EBS. Le suivi et la gestion de vos dépenses sont essentiels pour optimiser vos coûts.

Les tableaux suivants décrivent les codes Amazon EBS qui apparaissent dans vos rapports de facturation et d'utilisation. Pour obtenir la liste des codes de région utilisés dans les rapports de facturation et d'utilisation, consultez la section [Codes de facturation des AWS](#).

Codes de facturation pour :

- [Instantanés](#)
- [Stockage de volume](#)
- [Performances provisionnées](#)
- [API directes EBS](#)
- [Restauration rapide des instantanés \(FSR\)](#)

Ressources connexes

- [Tarification Amazon EBS](#)
- [the section called “Tarification”](#)

Instantanés

Code	Description	Unités	Granularité
<i>region</i> - EBS:Snap shotUsage	Instantanés de niveau standard (copies incrémentielles).	GB-Month	Par heure

Code	Description	Unités	Granularité
<i>region</i> - EBS:SnapshotArchiveStorage	Instantanés au niveau de l'archivage (copies complètes).	GB-Month	Par heure
<i>region</i> - EBS:SnapshotArchiveEarlyDelete	Suppression des instantanés archivés avant la fin de la période de conservation minimale.	Go	Par suppression
<i>region</i> - EBS:SnapshotArchiveRetrieval	Récupération d'instantanés archivés.	Go	Par Go

Stockage de volume

Code	Description	Unités	Granularité
<i>region</i> - EBS:VolumeUsage.gp3	Stockage pour volumes SSD à usage général (gp3).	GB-Month	Par heure
<i>region</i> - EBS:VolumeUsage.gp2	Stockage pour les volumes SSD à usage général (g2).	GB-Month	Par heure
<i>region</i> - EBS:Volume	Stockage pour les volumes SSD IOPS provisionnés (io2).	GB-Month	Par heure

Code	Description	Unités	Granularité
<code>meUsage.io2</code>			
<i>region</i> - <code>EBS:VolumeUsage.iops</code>	Stockage pour les volumes SSD IOPS provisionnés (io1).	GB-Month	Par heure
<i>region</i> - <code>EBS:VolumeUsage.st1</code>	Stockage pour les volumes de disque dur à débit optimisé.	GB-Month	Par heure
<i>region</i> - <code>EBS:VolumeUsage.sc1</code>	Stockage pour les volumes Cold HDD.	GB-Month	Par heure
<i>region</i> - <code>EBS:VolumeUsage</code>	Stockage pour volumes magnétiques.	GB-Month	Par heure

Performances provisionnées

Code	Description	Unités	Granularité
<i>region</i> - <code>EBS:VolumeP-Throughput.gp3</code>	Débit provisionné pour les volumes gp3 supérieurs à 125. MB/s	MB/s-Month	Par heure
<i>region</i> - <code>EBS:Volume</code>	IOPS provisionné pour les volumes mp3 supérieurs à 3 000.	IOPS-Month	Par heure

Code	Description	Unités	Granularité
meP-IOPS. gp3			
<i>region</i> - EBS:Volu meP-IOPS. io2	IOPS provisionnées pour des volumes io2 allant jusqu'à 32 000.	IOPS-Month	Par heure
<i>region</i> - EBS:Volu meP-IOPS. io2.tier2	IOPS provisionnées pour les volumes io2 compris entre 32 001 et 64 000.	IOPS-Month	Par heure
<i>region</i> - EBS:Volu meP-IOPS. io2.tier3	IOPS provisionnées pour les volumes io2 supérieurs à 64 000.	IOPS-Month	Par heure
<i>region</i> - EBS:Volu meP-IOPS. piops	IOPS provisionnées pour les volumes io1.	IOPS-Month	Par heure
<i>region</i> - EBS:Volu meIOUsage	IOPS héritées.	IOPS-Month	Par heure

API directes EBS

Code	Description	Unités	Granularité
<i>region</i> - EBS:dire	Appels aux actions de l'ListSnapshots API ListChangedBlocks et de l'API.	Pour 1 000 demandes	Par demande

Code	Description	Unités	Granularité
ctAPI.snapshot.List			
<i>region</i> -EBS:directAPI.snapshot.Get	Blocs renvoyés par l'action de l'GetSnapshotBlock API.	Pour 1 000 blocs renvoyés	Par demande
<i>region</i> -EBS:directAPI.snapshot.Put	Blocs écrits par l'action de l'PutSnapshotBlock API.	Pour 1 000 blocs écrits	Par demande

Restauration rapide des instantanés (FSR)

Code	Description	Unités	Granularité
<i>region</i> -EBS:FastSnapshotRestore	Les services de données Unit-Hours (DSU-Hours) pour les instantanés sont activés pour une restauration rapide des instantanés (par AZ).	DSU-Hours	Par minute (minimum une heure)

Créez un inventaire de vos volumes EBS

Amazon EBS fournit des ressources de stockage par blocs évolutives et hautes performances qui peuvent être utilisées avec les instances EC2. Vous pouvez associer un volume EBS à une instance EC2. Vous pouvez également détacher un volume EBS d'une instance EC2.

Les principales caractéristiques du stockage EBS sont les suivantes. Un administrateur système peut obtenir des informations sur ces caractéristiques de vos ressources EBS et les utiliser pour configurer un stockage fonctionnellement équivalent pour les serveurs que vous exécutez sur site ou les serveurs d'un autre fournisseur de cloud. Un administrateur système peut également récupérer

les données stockées dans vos ressources EBS, puis les stocker sur site ou dans un espace de stockage auprès d'un autre fournisseur de cloud.

Caractéristiques	Description
Volumes	Un volume EBS est un périphérique de stockage durable au niveau des blocs que vous pouvez connecter à une instance, formater et monter.
I/O performance	Amazon EBS propose plusieurs types de volumes, qui diffèrent en termes de performances et de prix.
Contenu de vos volumes de données EBS	Le seul moyen d'accéder directement aux données d'un volume est de le faire depuis l'instance.
Instantanés	Un instantané EBS est une copie instantanée des données d'un volume EBS. Les instantanés sont stockés dans Amazon S3, dans des compartiments auxquels vous ne pouvez pas accéder directement.
Contenu de vos instantanés EBS	Vous pouvez lire les données de vos instantanés ou les utiliser pour créer des volumes.

Volumes

Lorsque vous créez un volume EBS, vous sélectionnez une zone de disponibilité pour ce volume. Vous devez associer un volume EBS à une instance EC2 dans la même zone de disponibilité. Vous pouvez créer des volumes lorsque vous lancez une instance EC2, ou les créer d'abord, puis les associer à une instance. Si un volume est attaché à une instance, son statut est `in-use`. Si un volume n'est pas attaché à une instance, son statut est le suivant `available`.

Pourquoi est-ce important

Les volumes racine EBS contiennent le système d'exploitation de vos instances EC2. Les volumes de données EBS peuvent contenir des données critiques pour l'entreprise. Vous pouvez répertorier vos volumes EBS dans toutes les régions et indiquer s'ils sont attachés à des instances EC2.

Pour obtenir un résumé de vos volumes EBS dans toutes les régions

Vous pouvez utiliser [Amazon EC2 Global View](#) pour répertorier vos volumes EBS dans toutes les régions.

1. Ouvrez la console Amazon EC2 Global View à <https://console.aws.amazon.com/ec2globalview/home> l'adresse.
2. Dans l'onglet Explorateur de régions, sous Résumé, vérifiez le nombre de ressources pour les volumes, qui inclut le nombre de volumes et le nombre de régions. Choisissez le texte souligné pour voir comment le nombre de volumes est réparti entre les régions.
3. Dans l'onglet Recherche globale, sélectionnez le filtre client Type de ressource = Volume. Vous pouvez filtrer davantage les résultats en spécifiant une région ou une balise.

Pour décrire les volumes EBS en cours d'utilisation

Utilisez la commande [describe-volumes](#). Vous devez exécuter cette commande dans chaque région où vous avez des volumes EBS. Le `--filters` paramètre étend les résultats aux volumes qui le sont in-use. Le `--query` paramètre affiche uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-volumes \
  --filters Name=status,Values=in-use \
  --query "Volumes[].[VolumeId,Size,Attachments[0].InstanceId]" \
  --output table
```

Voici un exemple de sortie. Les colonnes sont l'ID du volume, la taille du volume, l'ID de l'instance attachée et le nom du périphérique.

```
-----
|                               DescribeVolumes                               |
+-----+-----+-----+-----+
| vol-0992ee65bec96de19 | 8 | i-00a7d9ec76a46a49f | /dev/xvda |
| vol-04d631d22047db1cb | 30 | i-0b1bf24fd4f297ab9 | /dev/sda1 |
| ... |
| ... |
```

```
| vol-0b811be5cbd1425cc | 100 | i-0a8d998154b320257 | /dev/xvde |
+-----+-----+-----+-----+
```

Pour décrire les volumes EBS qui ne sont pas utilisés

Dans la commande précédente, modifiez le filtre pour rechercher les volumes dont l'état est `available` le suivant.

```
--filters Name=status,Values=available
```

Si un volume n'est pas utilisé, vous devez déterminer s'il contient les données dont vous avez besoin. Par exemple, vous pouvez supprimer des volumes créés à des fins de test ou pour résoudre un problème. Un volume peut également être disponible si le périphérique de blocage qui a attaché le volume à l'instance a été [configuré pour persister](#) après la fermeture de l'instance. Si tel est le cas, vérifiez si les données du volume sont toujours nécessaires.

I/O performance

Le type de volume que vous spécifiez pour un volume EBS détermine ses performances. Selon le type de volume, vous pouvez spécifier une combinaison de taille, d'IOPS et de débit pour vos volumes. Pour plus d'informations sur les IOPS et le débit maximum provisionnés pour chaque type de volume, consultez la section Types de volumes [Amazon EBS](#).

Pourquoi est-ce important

Après avoir déterminé les performances de vos volumes EBS, vous pouvez définir les spécifications minimales requises pour un stockage fonctionnellement équivalent.

Pour obtenir des informations sur les performances de vos volumes

Utilisez la [commande](#) `describe-volumes` pour décrire les performances de vos volumes en cours d'utilisation. Le `--query` paramètre affiche uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire. Pour plus d'informations sur EBS-optimized les performances, reportez-vous aux spécifications des types d'instances [Amazon EC2](#) dans le Guide des types d'instances Amazon EC2.

```
aws ec2 describe-volumes \
  --filters Name=status,Values=in-use \
  --query "Volumes[].[VolumeId,VolumeType,Iops,Throughput]" \
```

```
--output table
```

Voici un exemple de sortie. Les colonnes sont l'ID du volume, le type de volume, les IOPS et le débit (MiB/s).

```
-----
|                               DescribeVolumes                               |
+-----+-----+-----+-----+
| vol-0992ee65bec96de19 | gp3 | 3000 | 125 |
| vol-04d631d22047db1cb | gp2 | 100 | None |
| ... |
| ... |
| vol-0b811be5cbd1425cc | gp3 | 3000 | 125 |
+-----+-----+-----+-----+
```

Contenu de vos volumes de données EBS

Amazon EBS n'a pas accès aux données que vous stockez sur vos volumes EBS. Vous êtes responsable de la sauvegarde de vos volumes de données. Par exemple, vous pouvez créer des instantanés instantanés, appelés instantanés EBS.

Vous pouvez également vous connecter à vos instances EC2 et transférer des fichiers depuis vos volumes EBS vers votre propre ordinateur. De nombreux outils sont disponibles pour vous aider à le faire. Voici quelques exemples.

Pourquoi est-ce important

Si vos volumes EBS contiennent des données critiques, vous pouvez les copier vers un stockage fonctionnellement équivalent.

Pour transférer des fichiers depuis un volume attaché à une instance Linux

Connectez-vous à votre instance Linux et utilisez SCP. Pour plus d'informations, voir [Transférer des fichiers à l'aide du SCP](#).

Pour transférer des fichiers depuis un volume attaché à une instance Windows

Connectez-vous à votre instance Windows et utilisez le protocole RDP. Pour plus d'informations, voir [Transférer des fichiers à l'aide du protocole RDP](#).

Instantanés

Vous pouvez sauvegarder vos volumes de données EBS en créant des instantanés EBS. Vous pouvez créer des instantanés EBS à l'aide d'[Amazon EBS](#), d'[Amazon Data Lifecycle Manager](#) ou. [AWS Backup](#)

Pourquoi est-ce important

Si vos volumes EBS contiennent des données critiques, il est fort probable que vous créiez des sauvegardes sous la forme d'instantanés EBS. Vous pouvez consulter les instantanés les plus récents de vos volumes et vérifier qu'ils reflètent les données actuelles sur les volumes.

Pour décrire les instantanés d'un volume spécifique

Utilisez la commande [describe-snapshots](#). Le `--filters` paramètre étend les résultats à des instantanés pour le volume spécifié. Le `--query` paramètre affiche uniquement les champs spécifiés dans la sortie. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws ec2 describe-snapshots \
  --filters Name=volume-id,Values=vol-00622ef8c2ac8b762 \
  --query Snapshots[*].[SnapshotId,CompletionTime,Description] --output table
```

Voici un exemple de sortie. Les colonnes sont l'ID du cliché, la date d'achèvement et le fait que le volume soit chiffré ou non.

```
-----
|                               DescribeSnapshots                               |
+-----+-----+-----+-----+
| snap-0ad439c50efabb47c | 2024-07-12T03:36:27.952000+00:00 | False |
+-----+-----+-----+-----+
```

Contenu de vos instantanés EBS

Vous ne pouvez ni télécharger ni exporter le contenu d'un instantané EBS vers un autre format. Vous pouvez toutefois accéder aux données de vos instantanés en utilisant les API EBS directes ou en créant un volume EBS à partir de l'instantané et en transférant les fichiers.

Pourquoi est-ce important

Si vos volumes EBS contiennent des données critiques, il est fort probable que vous créiez des sauvegardes sous la forme d'instantanés EBS. Vous pouvez récupérer ces données et les copier dans un stockage fonctionnellement équivalent.

Option 1 : pour lire les données de vos instantanés

Utilisez les API <https://docs.aws.amazon.com/ebs/latest/userguide/ebs-accessing-snapshot.html> EBS Direct.

Option 2 : pour créer un volume à partir d'un instantané et transférer les données

1. Utilisez la commande [create-volume](#) pour créer un volume à partir de l'instantané.

```
aws ec2 create-volume \  
  --volume-type gp3 \  
  --snapshot-id snap-0ad439c50efabb47c \  
  --iops 6000 \  
  --availability-zone us-east-2b
```

2. Utilisez la [commande](#) `attach-volume` pour associer le volume à une instance.

```
aws ec2 attach-volume \  
  --device /dev/sdf \  
  --instance-id i-0b1bf24fd4f297ab9 \  
  --volume-id vol-1234567890abcdef0
```

3. Connectez-vous à votre instance, [formatez et montez](#) le volume.
4. [Transférez les fichiers du volume](#) sur votre propre ordinateur.

Quotas pour Amazon EBS

Vous Compte AWS avez des quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota l'est Region-specific. Vous pouvez demander des augmentations de certains quotas, tandis que d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas pour Amazon EBS, ouvrez la console <https://console.aws.amazon.com/servicequotas/home> Service Quotas. Dans le volet de navigation, choisissez AWS services et sélectionnez Amazon Elastic Block Store (Amazon EBS). Pour demander une augmentation de quota, consultez [Demander une augmentation de quota](#) dans le Guide de l'utilisateur de Service Quotas.

Vous Compte AWS avez les quotas suivants liés à Amazon EBS.

Nom	Par défaut	Ajusté	Description
Instantanés archivés par volume	Chaque région prise en charge : 25	Oui	Le nombre maximum d'instantanés archivés par volume.
CompleteSnapshot demandes par compte	Chaque Région prise en charge : 10 par seconde	Non	Le nombre maximum de CompleteSnapshot demandes autorisées par compte.
Copies instantanées simultanées par région de destination	Chaque Région prise en charge : 20	Non	Le nombre maximum de copies simultanées d'instantanés vers une seule région de destination.
Instantanés simultanés par volume Cold HDD (sc1)	Par région prise en charge : 1	Non	Le nombre maximum de captures simultanées par volume Cold HDD (sc1) dans cette région.

Nom	Par défaut	Ajusté	Description
Instantanés simultanés par volume SSD à usage général (gp2)	Chaque région prise en charge : 5	Non	Le nombre maximum d'instantanés simultanés par volume SSD à usage général (gp2) dans cette région.
Instantanés simultanés par volume SSD à usage général (gp3)	Chaque région prise en charge : 5	Non	Le nombre maximum d'instantanés simultanés par volume SSD à usage général (gp3) dans cette région.
Instantanés simultanés par volume magnétique (standard)	Chaque région prise en charge : 5	Non	Le nombre maximum d'instantanés simultanés par volume magnétique (standard) dans cette région.
Instantanés simultanés par volume SSD IOPS provisionné (io1)	Chaque région prise en charge : 5	Non	Le nombre maximum d'instantanés simultanés par volume SSD IOPS provisionné (io1) dans cette région.
Instantanés simultanés par volume SSD IOPS provisionné (io2)	Chaque région prise en charge : 5	Non	Le nombre maximum d'instantanés simultanés par volume SSD IOPS provisionné (io2) dans cette région.
Instantanés simultanés par volume de disque dur à débit optimisé (st1)	Par région prise en charge : 1	Non	Nombre maximum de captures simultanées par volume de disque dur à débit optimisé (st1) dans cette région.

Nom	Par défaut	Ajuste	Description
Restauration d'instantané rapide	Chaque Région prise en charge : 5	Oui	Le nombre maximum d'instantanés pouvant être activés pour une restauration rapide des instantanés dans cette région.
GetSnapshotBlock demandes par compte	us-east-1 : 5 000 par seconde us-east-2 : 5 000 par seconde us-west-2 : 5 000 par seconde ap-southeast-1 : 5 000 par seconde eu-west-1 : 5 000 par seconde Chacune des autres régions prises en charge : 1 000 par seconde	Oui	Le nombre maximum de GetSnapshotBlock demandes autorisées par compte.
GetSnapshotBlock demandes par instantané	Chaque Région prise en charge : 1 000 par seconde	Non	Le nombre maximum de GetSnapshotBlock demandes autorisées par instantané.

Nom	Par défaut	Ajusté	Description
IOPS pour les volumes IOPS SSD (io1) provisionnés	Chaque région prise en charge : 300 000	Oui	Nombre agrégé maximum d'IOPS pouvant être provisionnées sur des volumes SSD IOPS provisionnés (io1) dans cette région.
IOPS pour les volumes IOPS SSD (io2) provisionnés	Chaque région prise en charge : 100 000	Oui	Nombre agrégé maximum d'IOPS pouvant être provisionnées sur des volumes SSD IOPS provisionnés (io2) dans cette région.
Modifications IOPS pour les volumes IOPS SSD (io1) provisionnés	Chaque région prise en charge : 500 000	Oui	Le nombre agrégé maximum d'IOPS qui peuvent être demandées dans le cadre de modifications de volume sur des volumes SSD IOPS provisionnés (io1) dans cette région.
Modifications IOPS pour les volumes IOPS SSD (io2) provisionnés	Chaque région prise en charge : 100 000	Oui	Le nombre maximal d'IOPS actuelles (depuis) et demandées (vers) pour les demandes de modification de volume sur les volumes SSD IOPS provisionnés (io2) de cette région.
In-progress archives d'instantanés par compte	Chaque région prise en charge : 25	Oui	Le nombre maximum d'archives de snapshots en cours par compte.

Nom	Par défaut	Ajuste	Description
In-progress restaurations d'instantanés à partir des archives par compte	Chaque Région prise en charge : 5	Oui	Le nombre maximum de restaurations d'instantanés en cours à partir des archives par compte.
ListChangedBlocks demandes par compte	Chaque région prise en charge : 50 par seconde	Non	Le nombre maximum de ListChangedBlocks demandes autorisées par compte.
ListSnapshotBlocks demandes par compte	Chaque région prise en charge : 50 par seconde	Non	Le nombre maximum de ListSnapshotBlocks demandes autorisées par compte.
Volume maximum de copies simultanées effectuées par compte	Chaque Région prise en charge : 5	Oui	Nombre maximum d'opérations simultanées de volumes de copies autorisées par compte dans cette région.
Taux provisionné pour l'initialisation des volumes pour les demandes de création de volumes simultanées par région	Chaque région prise en charge : 5 000	Oui	Taux provisionné agrégé maximum pour l'initialisation des volumes, en MiB/s, qui peut être demandé lors de demandes de création de volumes simultanées dans cette région.

Nom	Par défaut	Ajuste	Description
PutSnapshotBlock demandes par compte	us-east-1 : 5 000 par seconde us-east-2 : 5 000 par seconde us-west-2 : 5 000 par seconde ap-southeast-1 : 5 000 par seconde eu-west-1 : 5 000 par seconde Chacune des autres régions prises en charge : 1 000 par seconde	Oui	Le nombre maximum de PutSnapshotBlock demandes autorisées par compte.
PutSnapshotBlock demandes par instantané	Chaque Région prise en charge : 1 000 par seconde	Non	Le nombre maximum de PutSnapshotBlock demandes autorisées par instantané.
Instantanés par région	Chaque région prise en charge : 100 000	Oui	Le nombre maximum de clichés par région.
StartSnapshot instantanés en attente par compte	Chaque région prise en charge : 100	Non	Le nombre maximum de clichés en attente par compte qui peuvent être créés à l'aide de l' StartSnapshot API.

Nom	Par défaut	Ajuste	Description
StartSnapshot demandes par compte	Chaque Région prise en charge : 10 par seconde	Non	Le nombre maximum de StartSnapshot demandes autorisées par compte.

Nom	Par défaut	Ajuste	Description
Stockage des volumes Cold HDD (sc1), en TiB	États-Unis-est-1 : 50	Oui	Quantité de stockage agrégée maximale, en TiB, qui peut être provisionnée sur les volumes Cold HDD (sc1) de cette région.
	États-Unis-est-2 : 50		
	États-Unis-ouest-1 : 50		
	États-Unis-ouest-2 : 50		
	ap-nord-est-1 : 50		
	ap-nord-est-2 : 50		
	ap-sud-1 : 50		
	ap-sud-est-1 : 50		
	ap-sud-est-2 : 50		
	ca-central-1 : 50		
	eu-central-1 : 50		
	UE-Nord-1 : 50		
	UE-Ouest-1 : 50		
	UE-Ouest-2 : 50		
	UE-Ouest-3 : 50		
	mer-est-1 : 50		
	Chacune des autres régions		

Nom	Par défaut	Ajuste	Description
	prises en charge : 300		

Nom	Par défaut	Ajuste	Description
Stockage pour les volumes SSD à usage général (gp2), en TiB	États-Unis-est-1 : 50 États-Unis-est-2 : 50 États-Unis-ouest-1 : 50 États-Unis-ouest-2 : 50 ap-nord-est-1 : 50 ap-nord-est-2 : 50 ap-sud-1 : 50 ap-sud-est-1 : 50 ap-sud-est-2 : 50 ca-central-1 : 50 eu-central-1 : 50 UE-Nord-1 : 50 UE-Ouest-1 : 50 UE-Ouest-2 : 50 UE-Ouest-3 : 50 mer-est-1 : 50 Chacune des autres régions	Oui	Quantité de stockage agrégée maximale, en TiB, qui peut être provisionnée sur les volumes SSD à usage général (gp2) de cette région.

Nom	Par défaut	Ajusté	Description
	prises en charge : 300		
Stockage pour les volumes SSD à usage général (gp3), en TiB	Sud-1 : 300 ap-est-1 : 300 ap-est-2 : 300 ap-nord-est-3 : 300 ap-sud-2 : 300 ap-sud-est-4 : 300 ap-sud-est-5 : 300 ap-sud-est-6 : 300 ap-sud-est-7 : 300 centre-ouest : 300 eu-central-2 : 300 UE-Sud-1 : 300 UE-Sud-2 : 300 il-central-1 : 300 mx-central-1 : 300 Chacune des autres régions prises en charge : 50	Oui	Quantité de stockage agrégée maximale, en TiB, qui peut être provisionnée sur les volumes SSD à usage général (gp3) de cette région.

Nom	Par défaut	Ajuste	Description
Stockage pour volumes magnétiques (standard), en TiB	États-Unis-est-1 : 50 États-Unis-est-2 : 50 États-Unis-ouest-1 : 50 États-Unis-ouest-2 : 50 ap-nord-est-1 : 50 ap-nord-est-2 : 50 ap-sud-1 : 50 ap-sud-est-1 : 50 ap-sud-est-2 : 50 ca-central-1 : 50 eu-central-1 : 50 UE-Nord-1 : 50 UE-Ouest-1 : 50 UE-Ouest-2 : 50 UE-Ouest-3 : 50 mer-est-1 : 50 Chacune des autres régions	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être provisionnée sur les volumes magnétiques (standard) de cette région.

Nom	Par défaut	Ajuste	Description
	prises en charge : 300		

Nom	Par défaut	Ajusté	Description
Stockage pour les volumes IOPS SSD (io1) provisionnés, en TiB	États-Unis-est-1 : 50	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être provisionnée sur les volumes SSD IOPS provisionnés (io1) de cette région.
	États-Unis-est-2 : 50		
	États-Unis-ouest-1 : 50		
	États-Unis-ouest-2 : 50		
	ap-nord-est-1 : 50		
	ap-nord-est-2 : 50		
	ap-sud-1 : 50		
	ap-sud-est-1 : 50		
	ap-sud-est-2 : 50		
	ca-central-1 : 50		
	eu-central-1 : 50		
	UE-Nord-1 : 50		
	UE-Ouest-1 : 50		
	UE-Ouest-2 : 50		
	UE-Ouest-3 : 50		
	mer-est-1 : 50		
	Chacune des autres régions		

Nom	Par défaut	Ajuste	Description
	prises en charge : 300		
Stockage pour les volumes IOPS SSD (io2) provisionnés, en TiB	Chaque région prise en charge : 20	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être provisionnée sur les volumes SSD IOPS provisionnés (io2) de cette région.

Nom	Par défaut	Ajusté	Description
Stockage pour les volumes du disque dur (st1) à débit optimisé, en TiB	États-Unis-est-1 : 50	Oui	Quantité de stockage agrégée maximale, en TiB, qui peut être provisionnée sur les volumes de disque dur à débit optimisé (st1) dans cette région.
	États-Unis-est-2 : 50		
	États-Unis-ouest-1 : 50		
	États-Unis-ouest-2 : 50		
	ap-nord-est-1 : 50		
	ap-nord-est-2 : 50		
	ap-sud-1 : 50		
	ap-sud-est-1 : 50		
	ap-sud-est-2 : 50		
	ca-central-1 : 50		
	eu-central-1 : 50		
	UE-Nord-1 : 50		
	UE-Ouest-1 : 50		
	UE-Ouest-2 : 50		
	UE-Ouest-3 : 50		
	mer-est-1 : 50		
	Chacune des autres régions		

Nom	Par défaut	Ajusté	Description
	prises en charge : 300		
Modifications de stockage pour les volumes Cold HDD (sc1), en TiB	Chaque région prise en charge : 500	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être demandée lors de modifications de volume sur les volumes Cold HDD (sc1) de cette région.
Modifications de stockage pour les volumes SSD à usage général (gp2), en TiB	Chaque région prise en charge : 500	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être demandée en termes de modifications de volume sur les volumes SSD à usage général (gp2) de cette région.
Modifications de stockage pour les volumes SSD à usage général (gp3), en TiB	Chaque région prise en charge : 500	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être demandée en termes de modifications de volume sur les volumes SSD à usage général (gp3) de cette région.

Nom	Par défaut	Ajuste	Description
Modifications de stockage pour les volumes magnétiques (standard), en TiB	Chaque région prise en charge : 500	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être demandée en termes de modifications de volume pour les volumes magnétiques (standard) de cette région.
Modifications de stockage pour les volumes IOPS SSD (io1) provisionnés, en TiB	Chaque région prise en charge : 500	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être demandée en termes de modifications de volume sur les volumes Provisioned IOPS SSD (io1) de cette région.
Modifications de stockage pour les volumes IOPS SSD (io2) provisionnés, en TiB	Chaque région prise en charge : 20	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être demandée en termes de modifications de volume sur les volumes Provisioned IOPS SSD (io2) de cette région.

Nom	Par défaut	Ajustable	Description
Modifications de stockage pour les volumes du disque dur à débit optimisé (st1), en TiB	Chaque région prise en charge : 500	Oui	La quantité agrégée maximale de stockage, en TiB, qui peut être demandée dans le cadre de modifications de volume sur des volumes de disque dur à débit optimisé (st1) dans cette région.
Time-based débit de copies de snapshots par région de destination	Chaque Région prise en charge : 2 000	Oui	Débit maximal au niveau du compte, en MiB/sec, pour les opérations de copie de snapshots basées sur le temps par région de destination.

Considérations

- Vos quotas peuvent changer au fil du temps. Amazon EBS surveille en permanence votre stockage provisionné et votre utilisation des IOPS dans chaque région et peut augmenter automatiquement vos quotas, par région, en fonction de votre utilisation. Même si Amazon EBS peut augmenter automatiquement vos quotas en fonction de votre utilisation, vous pouvez demander une augmentation de quota si nécessaire. Par exemple, si vous prévoyez d'utiliser plus de gp3 stockage dans l'est des États-Unis (Virginie du Nord) que votre quota actuel, vous pouvez demander une augmentation du quota pour ce type de volume dans cette région avant votre utilisation prévue.
- Le quota de copies simultanées d'instantanés par région de destination n'est pas ajustable à l'aide des quotas de service. Vous pouvez toutefois demander une augmentation de ce quota en contactant le AWS support.
- Les quotas de modifications d'IOPS et de modifications de stockage s'appliquent à la valeur actuelle agrégée (pour la taille ou les IOPS, selon le quota) des volumes qui peuvent subir des modifications simultanément. Vous pouvez effectuer des demandes de modification simultanées pour des volumes dont la valeur actuelle combinée (pour la taille ou les IOPS) est supérieure

au quota. Par exemple, si votre quota de modifications IOPS pour les volumes d'IOPS SSD provisionnés (io1) est atteint 50,000, vous pouvez effectuer des demandes de modifications IOPS simultanées pour un nombre quelconque de io1 volumes tant que leurs IOPS actuelles combinées sont égales ou inférieures à 50,000. Si trois io1 volumes sont provisionnés avec des 20,000 IOPS chacun, vous pouvez demander des modifications IOPS pour deux volumes simultanément ($20,000 * 2 < 50,000$). Si vous soumettez une demande de modification d'IOPS simultanée pour le troisième volume, vous dépassez votre quota et cette demande échoue ($20,000 * 3 > 50,000$).

- Amazon EBS applique les limites non ajustables suivantes pour le nombre de volumes EBS par demande de lancement d'instance.
 - 2500— us-east-1, us-west-2, eu-west-1, et ap-northeast-1
 - 500— toutes les autres régions

Cette limite s'applique aux demandes de lancement d'instance que vous effectuez et aux demandes de lancement d'instance effectuées par AWS des services, tels qu'Amazon EMR, en votre nom. Si votre demande de lancement d'instance échoue en raison du dépassement de cette limite, ajustez la configuration du volume EBS dans la demande de lancement afin de réduire le nombre de volumes en dessous de la limite. Vous pouvez également contacter votre responsable technique des comptes (TAM) pour explorer d'autres options pour lancer votre cluster.

Historique des documents pour le guide de l'utilisateur Amazon EBS

Le tableau suivant décrit les versions de documentation relatives à Amazon EBS.

Modification	Description	Date
Mise à jour des modifications apportées à Elastic	Vous pouvez désormais initier une nouvelle modification d'Elastic Volumes dès que la précédente est terminée, jusqu'à quatre fois sur une période de 24 heures.	15 janvier 2026
Corbeille pour volumes EBS	La corbeille vous permet de protéger les volumes Amazon EBS contre les suppressions accidentelles.	20 novembre 2025
Copier un volume EBS	Vous pouvez créer une copie instantanée et instantanée d'un volume Amazon EBS au sein de la même zone de disponibilité.	14 octobre 2025
mises à jour des volumes GP3	Vous pouvez désormais provisionner des volumes SSD à usage général (gp3) d'une taille allant jusqu'à 64 TiB, d'IOPS jusqu'à 80 000 et d'un débit allant jusqu'à 2 000. MiB/s	26 septembre 2025
Mises à jour des directives de latence pour les volumes io2	io2Les volumes Block Express sont conçus pour fournir une latence moyenne inférieure à 500 microseco	26 septembre 2025

ndes pour des opération
s de 16 Ko I/O . io2 Les
volumes Block Express offrent
également une meilleure
latence aux valeurs aberrante
s par rapport aux volumes à
usage général, réduisant ainsi
de plus de 10 fois la fréquence
des I/Os dépassements de
800 microsecondes.

[Injection de latence](#)

Utilisez l'action d'injection de
AWS FIS latence pour simuler
une I/O latence élevée sur vos
volumes Amazon EBS.

16 septembre 2025

[io2Expansion régionale](#)

Les volumes IOPS SSD (io2)
provisionnés sont désormais
disponibles dans tous les
magasins et AWS GovCloud
(US) toutes les régions.

22 juillet 2025

[Instantanés locaux dans les zones locales](#)

Vous pouvez désormais créer
des instantanés locaux dans
Local Zones.

15 mai 2025

[Tarif provisionné par Amazon EBS pour l'initialisation des volumes](#)

Vous pouvez désormais
spécifier un taux d'initialisation
des volumes lorsque vous
créez des volumes Amazon
EBS afin de vous assurer
qu'ils sont entièrement initialis
és dans un laps de temps
prévisible.

6 mai 2025

Points de terminaison VPC Amazon Data Lifecycle Manager	Vous pouvez désormais établir une connexion privée entre votre VPC et Amazon Data Lifecycle Manager en créant un point de terminaison VPC d'interface.	28 février 2025
Time-based Exemplaires AMI	Vous pouvez désormais demander une durée d'exécution pour les opérations de copie d' EBS-backed AMI afin de vous assurer que les copies d'AMI sont terminées dans un délai précis.	25 février 2025
Taille complète de l'instantané	Vous pouvez désormais afficher la taille réelle d'un instantané Amazon EBS à l'aide de la console Amazon EC2 et. AWS CLI	11 février 2025
Prise en charge IPv6 d'Amazon Data Lifecycle Manager	Amazon Data Lifecycle Manager fournit désormais des points de terminaison à double pile qui prennent en charge le trafic IPv4 et IPv6.	7 février 2025
Support IPv6 pour la corbeille	La corbeille fournit désormais des points de terminaison à double pile qui prennent en charge à la fois le trafic IPv4 et IPv6.	19 décembre 2024
Instantanés locaux dans des zones locales dédiées	Vous pouvez désormais créer des instantanés locaux dans des zones locales dédiées.	16 décembre 2024

[AWSDataLifecycleManagerServiceRole AWS politique gérée mise à jour](#)

La politique AWSDataLifecycleManagerServiceRole AWS gérée a été mise à jour pour inclure l'autorisation pour l'ec2:DescribeAvailabilityZones action.

16 décembre 2024

[Politiques déclaratives pour bloquer l'accès public aux instantanés EBS](#)

Vous pouvez désormais utiliser des politiques déclaratives pour appliquer des paramètres au niveau du compte afin de bloquer l'accès public aux instantanés provenant de plusieurs régions et comptes simultanément. Pour plus d'informations, consultez la rubrique [Politiques déclaratives](#) dans le Guide de l'utilisateur AWS Organizations .

1er décembre 2024

[Time-based copies instantanées](#)

Vous pouvez désormais demander une durée d'exécution pour les opérations de copie d'instantanés afin de vous assurer que les copies d'instantanés sont terminées dans un délai précis.

26 novembre 2024

[Étiquettes d'exclusion pour corbeille](#)

Vous pouvez désormais ajouter des balises d'exclusion aux règles de Region-level rétention afin d'exclure les ressources qui possèdent des balises spécifiques.

19 novembre 2024

CloudFormation support pour Recycle Bin	Vous pouvez désormais créer et gérer des règles de conservation des corbeilles à l'aide de AWS CloudFormation.	18 novembre 2024
Statistiques de performances détaillées d'Amazon EBS	Les appareils en mode bloc Amazon EBS NVMe fournissent des statistiques de I/O performances haute résolution en temps réel pour les volumes Amazon EBS attachés aux Nitro-based instances Amazon EC2.	12 novembre 2024
Nouvelles CloudWatch mesures pour les volumes Amazon EBS	Vous pouvez désormais utiliser les CloudWatch métriques VolumeAvgReadLatency, VolumeAvgWriteLatency, VolumeIOPSExceededCheck, et VolumeThroughputExceededCheck Amazon pour surveiller les performances des volumes.	30 octobre 2024
Activez les politiques par défaut d'Amazon Data Lifecycle Manager pour tous les comptes	Vous pouvez les utiliser CloudFormation StackSets pour activer les politiques par défaut d'Amazon Data Lifecycle Manager au sein d'une AWS organisation ou pour des AWS comptes spécifiques.	26 avril 2024

[AWSDataLifecycleManagerSSMFullAccess AWS stratégie gérée](#)

Mise à jour de la politique afin de prendre en charge les instantanés cohérents par rapport à l'application pour SAP HANA à l'aide du document SSM AWS Systems Manager SAP-CreateDLMSnapshotForSAPHANA .

17 novembre 2023

[VolumeStalledIOCheck métrique](#)

Vous pouvez utiliser la métrique VolumeStalledIOCheck pour vérifier si un volume a réussi ou échoué à une vérification d'E/S bloquée au cours de la dernière minute.

16 novembre 2023

[Politiques par défaut Amazon Data Lifecycle Manager](#)

Vous pouvez désormais créer des politiques par défaut d'Amazon Data Lifecycle Manager pour les instantanés EBS et les EBS-backed AMI afin de sauvegarder tous les volumes et instances d'une région.

16 novembre 2023

[Verrouillage d'instantanés Amazon EBS](#)

Vous pouvez verrouiller vos instantanés Amazon EBS pour les protéger contre les suppressions accidentelles ou malveillantes, ou pour les stocker au format WORM pendant une durée déterminée.

15 novembre 2023

Blocage de l'accès public pour les instantanés	Vous pouvez désormais activer le blocage de l'accès public pour les instantanés pour empêcher le partage public de vos instantanés.	9 novembre 2023
Pré-scripts et post-scripts Amazon Data Lifecycle Manager	Vous pouvez désormais utiliser les pré-scripts et les post-scripts dans vos politiques d'instantanés Amazon Data Lifecycle Manager pour automatiser le cycle de vie des instantanés cohérents par rapport à l'application.	7 novembre 2023
Réservations NVMe	Multi-Attach io2 les volumes activés prennent en charge les réservations NVMe, qui est un ensemble de protocoles de séparation de stockage standard.	18 septembre 2023
Tests de défaillance sur Amazon EBS	Utilisez cette AWS FIS option pour vous arrêter temporairement I/O entre un volume EBS et les instances auxquelles il est attaché afin de tester la manière dont vos charges de travail gèrent I/O les interruptions.	27 janvier 2023
Verrouillage d'une règle de conservation de la corbeille	Vous pouvez verrouiller vos règles de conservation pour les protéger contre les modifications et les suppressions accidentelles ou malveillantes.	23 novembre 2022

Clés de condition pour la corbeille	Vous pouvez utiliser les clés de condition <code>rbn:Request/ResourceType</code> et <code>rbn:Attribute/ResourceType</code> pour filtrer l'accès sur les demandes de corbeille.	14 juin 2022
Volumes io2 Block Express	Vous pouvez modifier la taille et les IOPS provisionnés des volumes io2 Block Express et vous pouvez les activer pour une restauration rapide des instantanés.	31 mai 2022
Corbeille pour AMI	La corbeille vous permet de restaurer les AMI supprimées accidentellement.	3 février 2022
Corbeille pour instantanés Amazon EBS	La corbeille des instantanés Amazon EBS est une fonction de récupération d'instantanés qui vous permet de restaurer des instantanés supprimés accidentellement.	29 novembre 2021
Amazon EBS Snapshots Archive	Amazon EBS Snapshots Archive est un nouveau niveau de stockage que vous pouvez utiliser pour le stockage à long terme et à faible coût de vos instantanés rarement consultés.	29 novembre 2021

Prise en charge de l'obsolescence des AMI pour Amazon Data Lifecycle Manager	Les politiques EBS-backend d'AMI d'Amazon Data Lifecycle Manager peuvent rendre les AMI obsolètes . La politique AWSDataLifecycleManagerServiceRoleForAMIManagement AWS gérée a été mise à jour pour prendre en charge cette fonctionnalité.	23 août 2021
CloudWatch mesures pour Amazon Data Lifecycle Manager	Vous pouvez surveiller vos politiques Amazon Data Lifecycle Manager à l'aide d'Amazon CloudWatch.	28 juillet 2021
CloudTrail événements de données pour les API EBS Direct	Les ListSnapshotBlocks événements ListChangedBlocks de GetSnapshotBlock données peuvent être enregistrés dans les PutSnapshotBlock API,, et CloudTrail.	27 Juillet 2021
Volumes io2 Block Express	io2Les volumes Block Express sont désormais disponibles pour tous.	19 juillet 2021
Instantanés locaux Amazon EBS sur Outposts	Vous pouvez désormais utiliser les instantanés locaux d'Amazon EBS sur Outposts pour stocker des instantanés des volumes sur et Outpost localement dans Amazon S3 sur lui-même. Outpost	4 février 2021

<u>Multi-Attach prise en charge des volumes io2</u>	Vous pouvez désormais activer les volumes SSD IOPS provisionnés (io2) pour Amazon EBS. Multi-Attach	18 décembre 2020
<u>Amazon Data Lifecycle Manager</u>	Utilisez Amazon Data Lifecycle Manager pour automatiser le processus de partage des instantanés et de leur copie sur plusieurs AWS comptes.	17 décembre 2020
<u>Volumes gp3</u>	Un nouveau type de volume Amazon EBS SSD à usage général. Vous pouvez spécifier le débit et les IOPS provisionnés lorsque vous créez ou modifiez le volume.	1er décembre 2020
<u>Tailles de volume HDD à débit optimisé et HDD à froid</u>	Les volumes HDD à débit optimisé (st1) et HDD à froid (sc1) peuvent varier de 125 GiO à 16 TiO.	30 novembre 2020
<u>Amazon Data Lifecycle Manager</u>	Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création, la conservation et la suppression des EBS-backed AMI.	9 novembre 2020
<u>Amazon Data Lifecycle Manager</u>	Les politiques Amazon Data Lifecycle Manager peuvent être configurées avec quatre planifications au maximum.	17 septembre 2020

[Volumes SSD IOPS \(io2\) provisionnés pour Amazon EBS](#)

Les volumes (io2) SSD d'IOPS provisionnés sont conçus pour offrir une durabilité de volume de 99,999 % avec un AFR ne dépassant pas 0,001 %.

24 août 2020

[Restauration d'instantané rapide](#)

Vous pouvez activer la restauration rapide des instantanés pour les instantanés partagés avec vous.

21 juillet 2020

[Amazon EBS Multi-Attach](#)

Vous pouvez désormais associer un seul volume SSD IOPS provisionné (io1) à un maximum de 16 Nitro-based instances situées dans la même zone de disponibilité.

14 février 2020

[Restaurations d'instantanés rapides Amazon EBS](#)

Vous pouvez activer la restauration rapide des instantanés sur un instantané EBS pour vous assurer que les volumes EBS créés à partir de l'instantané sont entièrement initialisés lors de la création et fournissent instantanément toutes les performances prévues.

20 novembre 2019

[Instantanés multi-volumes Amazon EBS](#)

Vous pouvez prendre des instantanés en lien avec la panne, aux données coordonnées et à un instant donné exact, sur plusieurs volumes EBS attachés à une instance EC2.

29 mai 2019

Chiffrement Amazon EBS par défaut	Une fois que vous avez activé le chiffrement par défaut dans une région, tous les nouveaux volumes EBS que vous créez dans cette région sont chiffrés à l'aide de la clé KMS par défaut pour le chiffrement EBS.	23 mai 2019
Automatisez le cycle de vie	Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création et la suppression d'instantanés pour vos volumes EBS.	12 juillet 2018
Effectuer des modifications sur les volumes EBS attachés	Avec la plupart des volumes EBS attachés à la plupart des instances EC2, vous pouvez modifier la taille de volume, le type et les IOPS sans détacher le volume, ni arrêter l'instance.	13 février 2017
Copiez des instantanés Amazon EBS chiffrés entre Comptes AWS	Vous pouvez désormais copier des instantanés EBS chiffrés entre les deux. Comptes AWS	21 juin 2016
Types de volumes de disque dur à débit optimisé et de disque dur froid	Vous pouvez désormais créer des volumes HDD à débit optimisé (st1) et des volumes HDD à froid (sc1).	19 avril 2016

[Type de volume SSD à usage général](#)

Les volumes SSD à usage général offrent un stockage économique idéal pour un large éventail de charges de travail. Ces volumes offrent des latences en millisecondes à un chiffre, la capacité d'atteindre 3 000 IOPS pendant de longues périodes et une performance de base de 3. IOPS/GiB La taille des volumes polyvalents peut aller de 1 Gio à 1 Tio.

16 juin 2014

[Chiffrement Amazon EBS](#)

Chiffrement Amazon EBS offre un chiffrement transparent des instantanés et des volumes de données EBS sans que vous ayez à développer et à maintenir une infrastructure de gestion de clés sécurisée. Le chiffrement EBS assure la sécurité des données au repos en chiffrant vos données à l'aide de clés Clés gérées par AWS. Le chiffrement est effectué sur les serveurs hébergeant des instances EC2, assurant le chiffrement des données lorsqu'elles se déplacent entre les instances EC2 et le stockage EBS.

21 mai 2014

[Copies instantanées incrémentielles](#)

Vous pouvez désormais effectuer des copies d'instantané incrémentielles.

11 juin 2013

[Copie instantanée EBS](#)

Vous pouvez utiliser les copies d'instantané pour créer des sauvegardes de données, des volumes Amazon EBS ou des Amazon Machine Images (AMI).

17 décembre 2012

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.